FORE Systems
ES-2810 Ethernet Switch
User's Manual

MANU0330-02 - Rev. A - November, 1998

Firmware Version 2.31

Stack View Version 2.00

FORE Systems, Inc.

1000 FORE Drive

Warrendale, PA 15086-7502

Phone: 724-742-4444

FAX: 724-772-6500

URL: http://www.fore.com

Legal Notices

U.S. Government Restricted Rights. If you are licensing the Software on behalf of the U.S. Government ("Government"), the following provisions apply to you. If the Software is supplied to the Department of Defense ("DoD"), it is classified as "Commercial Computer Software" under paragraph 252.227-7014 of the DoD Supplement to the Federal Acquisition Regulations ("DFARS") (or any successor regulations) and the Government is acquiring only the license rights granted herein (the license rights customarily provided to non-Government users). If the Software is supplied to any unit or agency of the Government other than DoD, it is classified as "Restricted Computer Software" and the Government's rights in the Software are defined in paragraph 52.227-19 of the Federal Acquisition Regulations ("FAR") (or any successor regulations) or, in the cases of NASA, in paragraph 18.52.227-86 of the NASA Supplement to the FAR (or any successor regulations).

FCC CLASS A NOTICE

WARNING: Changes or modifications to this unit not expressly approved by the party responsible for compliance could void this user's authority to operate this equipment.

NOTE: The ES-2810 Ethernet Switch has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of the equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

CE NOTICE

Marking by the symbol **CE** indicates compliance of this system to the EMC (Electromagnetic Compatibility) directive of the European Community and compliance to the Low Voltage (Safety) Directive. Such marking is indicative that this system meets or exceeds the following technical standards:

- EN 55022 - "Limits and Methods of Measurement of Radio Interference Characteristics of Information Technology Equipment."
- EN 50082-1 - "Electromagnetic compatibility - Generic immunity standard Part 1: Residential, commercial, and light industry."
- IEC 1000-4-2 - "Electromagnetic compatibility for industrial-process measurement and control equipment Part 2: Electrostatic discharge requirements."
- IEC 1000-4-3 - "Electromagnetic compatibility for industrial-process measurement and control equipment Part 3: Radiate electromagnetic field requirements."
- IEC 1000-4-4 - "Electromagnetic compatibility for industrial-process measurement and control equipment Part 4: Electrical fast transient / burst requirements."
- IEC 1000-4-5 - "Electromagnetic compatibility - Generic immunity standard Part 5: Surge test."

CERTIFICATIONS

ETL certified to meet Information Technology Equipment safety standards UL 1950, CSA 22.2 No. 950, and EN 60950.

TRADEMARKS

Table of Contents

CHAPTER 4 Advanced Configuration

CHAPTER 5 Managing the Switch

APPENDIX A Concepts in Switching

List of Figures

Preface

This manual provides the necessary information to install the FORE Systems ES-2810 Ethernet switch. Also included is general product, network configuration, and software administration information. This manual is for users with various levels of experience.

If you have any questions or problems with the installation, please contact FORE Systems' Technical Assistance Center (TAC) using the information on page ii.

Chapter Summaries

Chapter 1 - Introduction to the ES-2810 - Provides an overview of the ES-2810 switch and installation procedures for the switch and its modules.

Chapter 2 - FORE Stack View - Provides an overview of the Stack View network management software for the ES-2810.

Chapter 3 - Standard Configuration - Provides information on doing a standard configuration of the ES-2810.

Chapter 4 - Advanced Configuration - Provides information on doing an advanced configuration using virtual LANs (VLANs).

Chapter 5 - Managing the Switch - Provides information on managing the ES-2810 using the Stack View network management software.

Chapter 6 - Technical Specifications - Provides physical, power and performance specifications for the ES-2810 and its modules.

Chapter 7 - Console Port Use and Troubleshooting - Provides information about using the switch's console port for local management and maintenance and a troubleshooting checklist for the ES-2810.

Appendix A - Concepts in Switching - Provides a basic overview of switching concepts including forwarding modes, flow control, filtering, IP, etc.

Technical Support

In the U.S.A., you can contact FORE Systems' Technical Assistance Center (TAC) using any one of the following methods:

1. You can receive on-line support via TACtics On-line at:

   http://www.fore.com/tac

2. You can contact Technical Support via e-mail at:

   support@fore.com

3. You can telephone your questions to Technical Support at:

   1-800-671-FORE (3673) or **+1 724-742-6999**

4. You can FAX your questions to Technical Support at:

   +1 724-742-7900

Technical support for non-U.S.A. customers should be handled through your local distributor.

No matter which method is used for support, please be prepared to provide your support contract ID number, the serial number(s) of the product(s), and as much information as possible describing your problem / question.

Typographical Styles

Throughout this manual, specific commands to be entered by the user appear on a separate line in bold typeface. In addition, use of the `Enter` or `Return` key is represented as `<ENTER>`. The following example demonstrates this convention:

`cd /usr <ENTER>`

Commands or file names that appear within the text of this manual are represented in the following style: "...the **`fore_install`** program will install this distribution"

As in the following example, any messages appearing on your screen during software installation and network interface administration will appear in `Courier` font to distinguish them from the rest of the text.

```
.... Are all four conditions true?
```

Important Information Indicators

To call your attention to important information that must be reviewed to ensure correct and complete installation, as well as to avoid problems with your software, FORE Systems utilizes the following *CAUTION/NOTE* indicators.

Information contained in **CAUTION** statements is important for proper installation/operation. **CAUTION** statements can prevent possible equipment damage and/or loss of data and will be indicated as:

CAUTION

You risk damaging your equipment and/or software if you do not follow these instructions.

Information contained in **NOTE** statements has been found important enough to be called to the special attention of the operator and will be set off from the text as follows:

FORE Systems strongly recommends that you disconnect the serial cable once you have configured the *ForeRunner* switch and then access the *ForeRunner* switch over the ATM network.

CHAPTER 1 Introduction to the ES-2810

This chapter covers the topics described in Table 1.1.

Table 1.1 - Topics Discussed in this Chapter

Topic	See Page
Introduction to the product	page 1-2
Front Panel	page 1-4
Rear Panel	page 1-6
Installation	page 1-7

1.1 Introduction to the product

1.1.1 Purpose of the Switch

The ES-2810 uses your existing network cables to integrate switching technology into your computer network.

Each device in a workgroup or a network segment can communicate at a full wire-speed of 10Mbps or 100Mbps to provide:

- High-speed connectivity
- Simultaneous two-way communication between connected devices
- Increased network throughput and performance
- Increased server availability

1.1.2 Physical Features

This switch offers the following features:

- Plug-and-play—no need to configure the module to use the basic operations
- 24 x 10/100Mbps connections
- Two option slots for modules
- Front panel LEDs that show switch, port and traffic status
- Automatic detection of 110V and 240V power supplies

1.1.3 Hardware Features

The switch offers the following features:

- Each port can operate in one of three switching modes: cut-through, fragment-free or store-and-forward
- Each port supports half- and full-duplex operation
- Simultaneous full wire-speed switching on all ports
- RMON support for Statistics, History, Alarm and Events
- Spanning tree support on all ports
- Flow control
- Permanent MAC address entries

1.1.4 Software Features

The switch offers the following features:

- FORE Stack View for Windows* 95, Windows* 98 and Windows NT* or FORE Stack View for Web
- Adaptive forwarding mode
- Local Management via a direct terminal connection or via TELNET
- SNMP Management support
- BOOTP and TFTP support
- Control over user access rights
- Creation of virtual LANs
- Stand-alone (per switch or stack) or distributed (switch network) VLAN
- IGMP Pruning

1.2 Front Panel

1.2.1 Introduction

The LEDs on the front panel show the status of the ports, so you should position the switch with the front panel facing you. You can also see which ports the cables are connected to on the switch.

1.2.2 View of the Front Panel

The front panel of the switch is shown below:

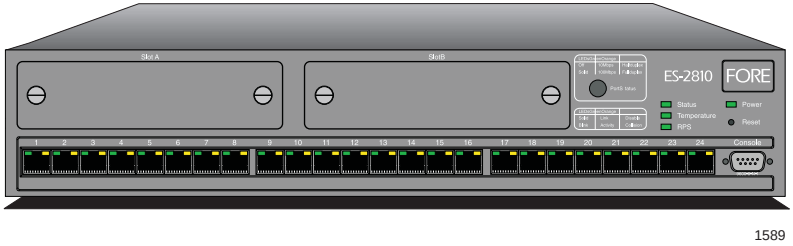


Figure 1.1 - The Front Panel of the ES-2810

1.2.3 Front Panel Ports

These ports are on the front panel:

Table 1.2 - Front Panel Ports

Port	Function
CONSOLE port (DB-9)	Connects a PC (running a VT100 emulation), a VT100 terminal or a modem to access the built-in Local Management program.
24 x 10/100Base-TX ports (RJ-45)	Connects devices using Unshielded Twisted Pair (UTP) cabling complying to EIA 568A Category 5 or ISO/IEC 11801 Category 5 level D.

1.2.4 Slots for Media Modules

After removing one or both of the cover plates, the modules can be inserted to expand the functionality of the switch.

1.2.5 Front Panel LED Functions

The LEDs on the front panel have the following functions:

Table 1.3 - Front Panel LEDs

LED	Shows the status for...
Port LEDs - Green and Orange	The operation of each port.
Status	The operation of the switch.
Power	The internal power supply.
Temperature	The internal temperature.
RPS (redundant power supply)	The external, redundant power supply.

1.2.6 Buttons

The buttons on the front panel have the following functions:

Table 1.4 - Front Panel Buttons

Button name	Function
Port Status	Shows the operational status of each port.
Reset	Reset or enter Maintenance Mode or Recovery Mode

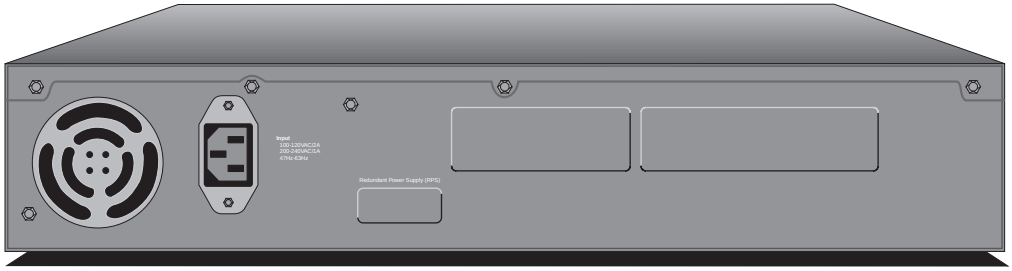
1.3 Rear Panel

1.3.1 Introduction

The rear panel has a cooling fan outlet and the main supply cable, so you should position the switch with the rear panel facing away from you.

1.3.2 View of Rear Panel

The rear panel of the switch is shown below:



1741

Figure 1.2 - Rear Panel of the ES-2810

1.3.3 Rear Panel Parts

The switch's rear panel has the following parts:

Table 1.5 - Rear Panel Components

Part	Function
Fan outlet	Cools the internal circuitry of the switch.
Power connection	A socket to connect the power cord to the main supply.
Redundant power supply connector	Connects an external redundant power supply. If the internal power supply fails, the redundant power supply starts immediately.

1.4 Installation

1.4.1 Important

You must adhere to all local and national regulations governing the installation and connection of electrical devices when installing the switch.

1.4.2 Before Installation

1.4.2.1 Contents of the Pack

Unpack the switch carefully and check that these parts are present:

Table 1.6 - Package Contents Checklist

Item	Present?
One ES-2810	
One power cord (suitable for your power outlet)	
One mounting kit	
One CD-ROM	
One Console cable	
One Quick Start	
FORE Documentation CD (including this on-line manual)	
FORE Release Notes	

1.4.2.2 Check the Package Contents

If you have not received all of the parts, or any of the parts are damaged, contact your dealer immediately.

Keep all the packaging materials in case you need to repack the switch.

1.4.2.3 Check All Labels

Read all labels and rating plates on the switch. If there is anything that you do not understand, or if any of the information provided does not appear to comply with your local or national rules and regulations, consult your dealer before proceeding with the installation.

1.4.2.4 Essential Reading

It is important that you read the following:

- Warnings and the instructions earlier in this guide.
- The Release Notes included with the switch.
- The `README.TXT` file on the CD-ROM. This gives a general description of the software and specific requirements.

1.5 Positioning and Installing the Switch

1.5.1 Allow Adequate Ventilation

The switch contains two fans to air-cool the internal circuitry. The air is drawn in from the left of the unit and expelled through the outlet grills on the right side and the rear.

To ensure correct airflow, leave 100 mm (4 inches) free space on both sides and behind the switch. Do not allow the intake or outlet grills to become blocked.

1.5.2 On a Desktop

To install the switch in a desktop environment:

1. Find the four rubber feet in the pack that contains the rack mounting kit.
2. Remove the backing strip from each of the four feet.
3. Attach the four rubber feet to the underside of the switch (to ensure that the switch stands firmly).
4. Place the switch on a stable, flat surface.
5. Ensure that the air intake (on the left) and fan outlets (on the right side and rear) are not blocked.

WARNING!

The switch's lifetime and operational reliability can be seriously degraded by inadequate cooling.

1.5.3 Rack Requirements

Install the switch in a standard rack in accordance with IEC 297 (or similar); if the minimum outside measurements of the rack are 600 x 600 mm (23.5 x 23.5 inches), you must allow 190 mm (7.5 inches) of space at the rear.

1.5.4 Mounting Kit

The switch is delivered with a kit to attach it to a standard 19-inch equipment rack (with side support rails). The kit contains two mounting brackets and four screws (for attaching the brackets to the sides of the switch).

1.5.5 Tools Required for Positioning in a Rack

In addition to the mounting kit, you need the following items to mount the switch in a rack:

- Standard 19-inch rack with side support rails.
- 3 mm screwdriver.
- Customer-supplied screws for securing the switch in the rack.

  Mounting screws are not provided because the required sizes may vary from rack to rack.

1.5.6 In an Equipment Rack

To mount the switch in a standard equipment rack:

1. Attach the mounting bracket marked “Left” to the left-hand side of the switch, and attach the mounting bracket marked “Right” to the right-hand side of the switch, using the four screws provided.

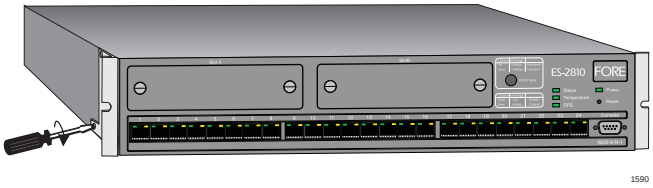


Figure 1.3 - Attaching the Mounting Brackets

   Make sure that you attach the mounting brackets to the correct sides. Otherwise the switch will not align correctly in the equipment rack.

2. If the four rubber feet prevent the switch from standing firmly on the equipment rack’s side support rails, remove them.
3. Set the switch in the equipment rack, and make sure there is adequate space for air flow around the switch (see “Allow Adequate Ventilation” on page 1-9).
4. Screw the mounting brackets securely to the equipment rack.

1.5.7 Ambient Temperature

If the switch is installed in a closed or multi-rack assembly, the operating ambient temperature of the rack environment may be greater than the ambient temperature of the room. Make sure that the temperature of the rack environment does not exceed the recommended operating temperature for the switch.

1.6 Installing a Module

1.6.1 Introduction

You can increase the connectivity options of your switch by installing a module.

WARNING!

Modules are not designed to be installed in, or removed from, the switch while it is in operation. You must power off the switch before attempting to install or remove a module.

1.6.2 Static-free Working Area

The module's printed circuit board is an Electrostatic Sensitive Device and should be handled only in a static-free working area; otherwise, the printed circuit board may fail or be degraded.

1.6.3 Avoiding Damage to the Circuit Board

If you remove the plate covering the slot on the front of the switch, for example, to install or remove a module, follow this procedure to avoid damage to your printed circuit board:

WARNING!

Do not remove the plate unless the switch is disconnected from the main power supply.

1. Disconnect the switch from the main power supply.
2. Ground the switch before you handle the printed circuit board.
3. Connect yourself to a non-painted / non-isolated part of the grounded switch (for example the back panel) using a wrist strap with 1MΩ resistance to ensure that you carry the same electrostatic charge as the enclosure.
4. Remove the plate covering the slot.

1.6.4 Installing a Module

To install a module:

1. If the switch is already operational, disconnect it from the main power supply.
2. Follow the instructions in "Avoiding damage to the circuit board" above.
3. Unscrew the screws of the plate covering the slot on the front of the switch. Save these screws and plate.
4. Insert the module into the slot. Place your thumbs just beneath the screws on the front panel of the module and push in the module. Secure it using the retaining screws.

1.6.5 Removing a Module

To remove a module:

1. If the switch is already operational, disconnect it from the main power supply.
2. Follow the instructions in "Avoiding damage to the circuit board" above.
3. Unscrew the screws securing the module.
4. Pull the module gently to disengage the connectors fully from the socket on the motherboard. Slide the module out completely.
5. Cover the empty module port with the plate and secure using the screws.

1.7 Connecting Other Devices

1.7.1 Introduction

Incorrect cabling is often the cause of network configuration problems

1.7.2 Use Shielded Cables

Shielded cables normally comply with EMC and FCC emission limits.

Only use unshielded cables when it is explicitly specified in the installation manual of the device in question.

1.7.3 Cables for the LAN Ports

Ports on the switch are wired MDI-X, so use the following cable:

Table 1.7 - LAN Port Cable Requirements

If you connect the switch to a...	Then use a...
Workstation or server	Straight-through cable 1:1
Device with MDI-X ports (for example another switch or hub)	Crossover cable
Device with MDI ports	Straight-through cable 1:1

1.7.4 RJ-45 Connector Pin Assignments

The RJ-45 ports on the front of the switch have the following pin assignments:

Table 1.8 - RJ-45 Connector Pinouts

Pin number	Function
1	RX+
2	RX-
3	TX+
6	TX-

1.7.5 Connecting a Device to the RJ-45 Ports

To connect a workstation compatible with IEEE 802.3 (Ethernet Version 1.0 and 2.0) or a fast access device (such as a server) to the switch's RJ-45 ports using UTP cable (Category 5):

1. Make sure that the device has a 100Mbps (100Base-FX or 10/100Base-TX) network interface card installed.

   If not, use your network interface card's documentation to install and configure it correctly.

2. If your workstation is fitted with an RJ-45 interface then there is no problem. However, it is possible to attach to other connector types using an appropriate adapter. For example, use a UTP/10Base-FL adapter for fiber connections
3. Connect one end of the UTP cable to an RJ-45 port on the switch.

   According to IEEE 802.3, the cable length must not exceed 100 meters (approximately 325 feet).

4. Connect the other end to the 100Base-TX connection on the device.

1.7.6 Cable for the Console Port

If you connect a PC (via the Console Port), then use a null-modem cable.

1.8 Connecting the Power

1.8.1 Introduction

After connecting the devices to the switch, connect the power cable. There are certain practical and safety considerations to be made before powering the switch on.

1.8.2 The Power Cable

1.8.2.1 Ground Warning

The switch is delivered with a power cable that fits the power sockets in your country. If this is not the case, contact your dealer immediately and ask for the correct power cable.

1.8.2.2 Power Cable Wiring Color Code

The wires in the power cable provided are color coded:

Table 1.9 - Color Codes for Power Cable Wiring

Color	Connection
Green and yellow	Ground
Blue	Neutral
Brown	Live

1.8.2.3 Important for UK Use

If the colors of the wires in the power cable provided do not correspond with the markings that identify the terminals in your plug:

1. Make sure that the green and yellow wire is connected to the terminal marked with the letter E, or with the ground symbol ⏚, or is colored green and yellow.
2. Make sure that the blue wire is connected to the terminal marked with the letter N or colored black.
3. Make sure that the brown wire is connected to the terminal marked with the letter L or colored red.

1.8.3 Power Supply to a Rack

If the switch is installed in a rack, make sure the rack's power supply socket has a ground connection and the rack is connected to a branch supply or a power supply socket with a ground connection.

To avoid overloading the circuit and damaging the wiring of the power supply, the power supply to the rack must be adequate to cover the extra power consumed by the switch.

1.9 Power Up

1.9.1 Powering Up the Switch

Follow these steps to power up the switch:

1. Push the female end of the power cable into the main socket (in the rear panel); plug the other end into the power supply outlet.
2. Make sure that the Power LED (on the front panel) is green.

   If it isn't green, make sure that the power outlet is working correctly (switched on). If the power outlet is on and the Power LED is not green, then there is a fault within the switch and you must contact your dealer.
3. Verify that an LED is lit for each of the front panel ports where a powered on device is connected.

1.9.2 Start-up Procedure

Immediately after power-up, the following should happen during start-up:

Table 1.10 - LED Indications During Start-up

Stage	STATUS LED...	Then the switch...
1	Is red	Is starting up
2	Turns to steady green	Has started successfully

If the Status LED remains red, then the switch has not started successfully. Try to restart it; if the switch does not start, contact your dealer.

Look at the other front panel LEDs during start-up and check that they are operating correctly.

1.9.3 Port LED States

The LEDs reflect the state of each port:

Table 1.11 - Port LED STatus Indications

LED	Indicates
No lights	Port enabled, no link.
Green, blinking randomly	Port enabled, Rx / Tx traffic, link pulse active.
Green, solid	Port enabled, link pulse active.
Green and Orange both blinking randomly	Collision detected (with half duplex). Port enabled, link pulse active.
Orange, solid	Port disabled by management.
Green and Orange both solid	Port disabled by a hardware fault, or no hardware connected.

1.9.4 Default Settings After Start-up

Once the switch has started successfully, installation is complete and the switch is using its default setting (also known as default configuration):

- All ports are enabled.
- All ports operate in auto-negotiation mode.
- Spanning Tree is disabled on all ports.
- Addresses that have been silent for more than 15 minutes are purged from the switch's address table (the MAC Address Aging time).
- No access restrictions to Local Management (Telnet).
- No SNMP restrictions.
- No permanent MAC address entries defined. A permanent entry is a MAC address that is defined as being permitted only on a certain port. This can be a useful security feature.
- All ports are in the same VLAN (named <System>) and VLAN mode (Stand-alone mode). VLANs allow you to create virtual networks using specific switch ports, IP addresses, IP subnets and MAC addresses.
- Flow Control is enabled on all ports.
- The connection with Local Management is timed-out after 10 minutes if there has been no input during this period.

1.9.5 After Start-up

This default configuration is adequate for simple workgroup environments to operate in basic switching mode.

Although the switch continues to operate without problems, we recommend that you change certain parameters to suit your own requirements.

Follow the instructions in Chapter 2 to change the configuration while the switch is operating.

1.10 Other LEDs on the Front Panel

1.10.1 Introduction

There are three other LEDs and one button on the front panel that show how the switch is operating:

- Status LED
- Temperature LED
- Redundant Power Supply (RPS) LED
- Port Status button

1.10.2 LED Colors and their Meanings

The LEDs give information about the state of the switch:

Table 1.12 - LED Indicator Colors and Meanings

LED	Color	Meaning
Status	Green	Solid: The switch is operating normally.
		Blinking (1 Hz): Updating software or running in recovery mode.
		Blinking (5 Hz): Running in maintenance mode.
	Red	The switch is resetting, or either hardware or software errors are detected.
Temperature	Green	Normal operating temperature.
	Orange	Temperature is higher than normal. Check that the area around the air intakes and vents are clear of obstructions.
	Red	Temperature is too high and the switch will shut down.
RPS	Green	Off: No RPS connected.
		Solid: RPS connected, but not needed.
	Orange	Normal power supply has failed and the RPS has taken over.

1.10.3 Port Status Button

To see the speed and duplex settings of all the ports, press the `Port Status` button. The function of the port LEDs changes for a period of 5 seconds, where they have the following meaning:

Table 1.13 - Port LED Indicator Colors and Meanings

LED	Color	Meaning
Left (Speed)	Green	Off: 10Mbps
		Solid: 100Mbps
Right (Duplex)	Orange	Off: Half duplex
		Solid: Full duplex

CHAPTER 2 FORE Stack View

2.1 In This Chapter

This chapter covers the topics described in Table 2.1.

Table 2.1 - Topics Discussed in this Chapter

2.2 System Requirements

2.2.1 Requirements for FORE Stack View under Windows

You need a PC with the following minimum requirements to run FORE Stack View:

- Microsoft Windows NT workstation or server, version 4.0, or Microsoft Windows 95 or Microsoft Windows 98. (Windows NT 4.0 English language version workstation recommended.)
- A network adapter.
- 30 MB of free hard disk space.
- A color display with 800 x 600 resolution and 256 colors.
- The Microsoft IP protocol must be installed and configured before installation of FORE Stack View.

2.2.2 DHCP Limitation

Three important things to know:

- Do not use a PC running Windows NT server (with its DHCP server installed) to run FORE Stack View.
- Ensure the IP address for the PC is not changed by the DHCP server.
- PCs that use a network management system that uses BootP, DHCP or SNMP Trap Receiving, may have their network management system disabled by FORE Stack View.

2.3 Installation and Removal

2.3.1 To start the installation of FORE Stack View

Normally, the Setup program for FORE Stack View will start automatically after you insert the compact disc (CD) in your CD ROM drive. However, if it does not, use the standard Windows procedures for installing programs. The screen shown in Figure 2.1 is displayed.

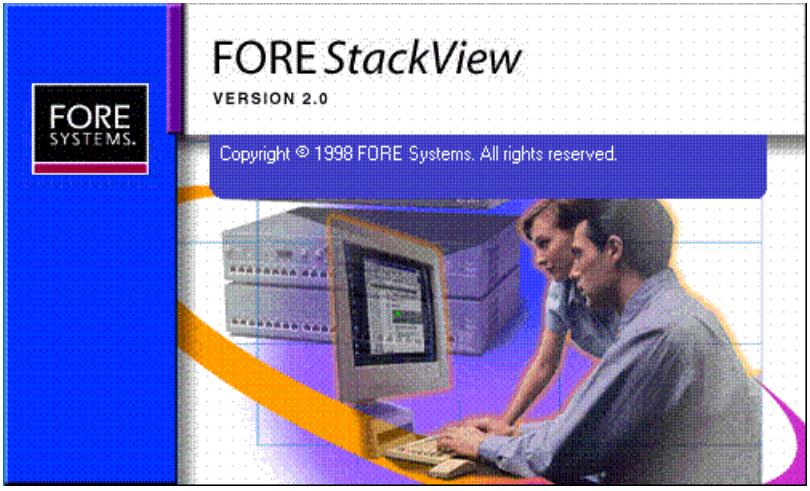


Figure 2.1 - The Start-up Screen for FORE Stack View Installation

2.3.2 To Install FORE Stack View for Windows

Click `Install Windows` and follow the on-screen instructions. When the installation is complete, FORE Stack View will start automatically when “Launch FORE Stack View” is selected.

2.4 Removal of FORE Stack View

2.4.1 Removal under Windows

To remove FORE Stack View under Windows:

1. Close all FORE Stack View programs.
2. Use standard Windows procedures to uninstall FORE Stack View.

2.5 Using FORE Stack View

2.5.1 Concept

FORE Stack View uses SNMP to configure all the parameters on your switch, or group of switches (known from here on as a stack), and monitors their activities.

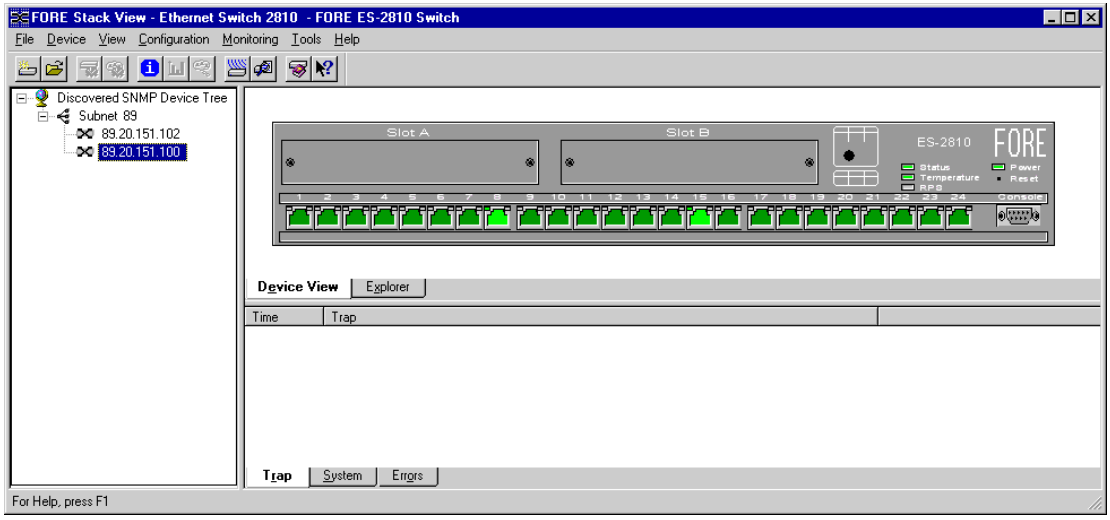


Figure 2.2 - FORE Stack View

2.5.2 Navigating through FORE Stack View

Many commands are available from within FORE Stack View. These are best accessed using mouse actions. However, Windows users can also access most of them through the menu bar.

2.5.3 The FORE Stack View Window

There are three sections:

- Device Tree — displays the separate branches on your LAN, including a branch showing all unconfigured devices.
- Interactive picture of the switch, or stack — shows the port state or the Explorer, which provides port and VLAN details for the switch or stack.
- Information section — provides details about diagnostics, traps, errors and the system. Using this window, you can show activity statistics for the switch (or the stack) and for individual ports.

2.6 Before a Switch is Contacted

2.6.1 Basic Menu Bar Commands

Before a switch or stack is contacted, the following commands are available through the menu bar. The toolbar buttons are for users using FORE Stack View in Windows.

2.6.2 File Menu

The File menu contains one command, Exit, which enables you to exit the FORE Stack View. When a switch or stack is open and the configuration has been changed and not saved to the Flash Memory as the permanent configuration, you are asked if you want to save the new configuration before exiting.

2.6.3 Device Menu

The Device menu contains the following switch commands:

- Install — enables you to install a new device, which does not have an IP address, in FORE Stack View. Can also be accessed by selecting  .
- Manage — enables a switch or stack that has an IP address already assigned to be managed or configured. Can also be accessed by selecting  .
- Discover — enables you to set up how the Device Tree discovers devices and users.
- A list of IP addresses — contains the last eight switches successfully contacted from FORE Stack View. These can be used to manage the switch.

2.6.4 View menu — for Windows Users Only

The View menu allows you to customize the FORE Stack View display to your own preferences: the Toolbar and Status Bar can be switched on and off.

2.6.5 Monitoring Menu

The Monitoring menu gives access to set the Default Preferences for FORE Stack View. See “Setting the Preferences” on page 2-10.

2.6.6 Tools Menu

The Tools menu has the following commands:

- Ping — Sends ICMP echo packets to the switch. Can also be accessed by selecting  .
- A Report Manager — Uploads reports, logs and the parameter block from the switch. Can also be accessed by selecting  .
- A Recovery Manager — Regains control of your switch if you have lost contact. This is described in “The Recovery Manager” on page 5-36.
- A DNS-IP conversion tool converts DNS names to IP addresses.

These are described in detail, together with switch specific tools, in Chapter 5.

2.6.7 Help Menu

The Help menu has the following commands for the switch:

- Help for FORE Stack View. Can also be accessed by selecting the Help icon  then clicking on the feature of interest
- Help for switch specific topics.

2.7 After a Switch or Stack is Contacted

2.7.1 Commands

When FORE Stack View contacts a switch, the basic commands are supplemented with:

- Local Management access — Provides Telnet access to monitoring functions embedded in the switch.
- RMON facility — Gathers information about the network traffic, monitors traffic on subnets and enables you to define alarms on the individual ports.
- Stack Synchronization Manager (for stacks only) — Enables you to establish a stack from a group of switches connected via a Matrix Module, or add a switch to an existing stack and then synchronize their configurations.
- Switch Position Organizer (for stacks only) — Enables you to move the switches displayed on screen around in the stack.
- Color Code Matrix Ports (for stacks only) — Colors the individual ports on the Matrix Module. This simplifies the task of tracing cables, as the ports on the Stack Interface Modules become the same color as the corresponding Matrix Module port.
- A color coding chart for FORE Stack View to show the states of switch's LEDs

2.8 Setting the Preferences

2.8.1 Setting the Polling Intervals

The polling intervals determine how often FORE Stack View contacts the switch or stack and updates the status and information displayed. To change the polling parameters:

1. Select `Monitoring>Preferences`.

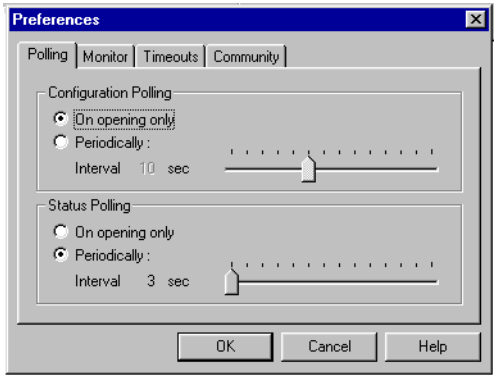


Figure 2.3 - Polling Tab of Preferences Dialog Box

2. Click `Polling` or `Monitor`.
3. If you want the polling to happen more frequently than just on opening, click `Periodically`.
4. Move the `Interval` slider to the required time.
5. Click `OK`.

2.8.2 Setting the Timeout Parameters for SNMP

The timeout determines the intervals between polling and the number of times the request is retried if a device is not responding. To change the timeout parameters:

1. Select `Monitoring>Preferences`.
2. Click `Timeouts`.

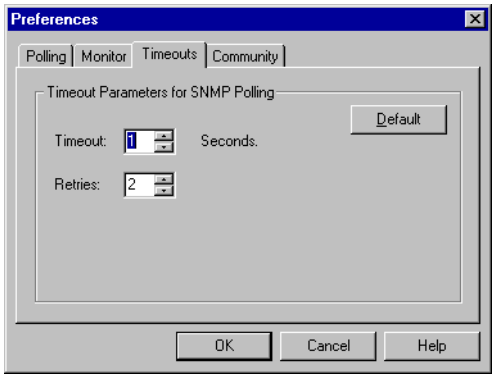


Figure 2.4 - Timeouts Tab of the Preferences Dialog Box

3. Change the values.
4. Click `OK`.

2.8.3 Setting the Community for SNMP Polling

The community for SNMP polling determines access rights. To change the community:

1. Select `Monitoring>Preferences`.
2. Click `Community`.

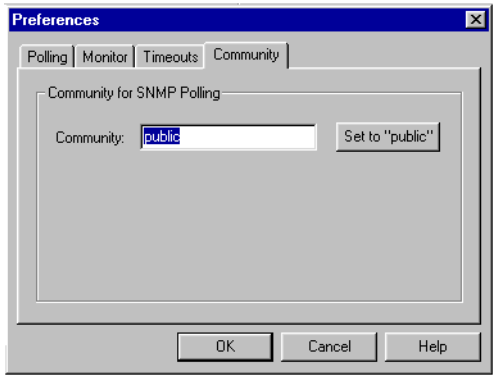


Figure 2.5 - Community Tab of the Preferences Dialog Box

3. Type the new community name.
4. Click `OK`.

2.9 Installing and Managing Switches

2.9.1 Following Installation of FORE Stack View

After installing FORE Stack View, you can add new switches, establish or expand stacks of switches, and manage existing switches and stacks.

2.9.2 Adding New Switches

To add new switches (that have not been assigned an IP address) to FORE Stack View, select `Device>Install`. The Install Wizard will start and guide you through the installation.

2.9.3 The Install Wizard

The Install Wizard requires that you enter a minimum amount of information to set up the switch for management by FORE Stack View. To select the correct new device, you need to know the device's MAC address. You can find this on a label on the rear panel of the device. You must assign an IP address (and subnet mask) to the switch on your Local Area Network (LAN). FORE Stack View uses this address for configuration and management purposes.

Figure 2.6 - The Install Wizard

2.9.4 Matrix Module Connected to a New Switch

When the Install wizard detects that a new switch is connected to a Matrix Module, a message (shown in Figure 2.7) informs that you must decide how to manage the switch.

- If you want to manage it separately, the installation is completed and the switch is displayed in the FORE Stack View window.
- If you want to manage it as part of a stack, you have the opportunity to assign consecutive IP addresses in the next dialog.

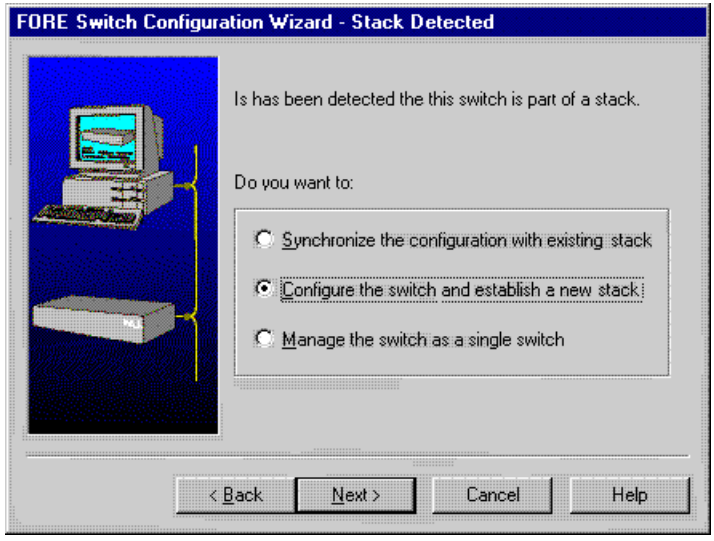


Figure 2.7 - Install Wizard New Switch Message

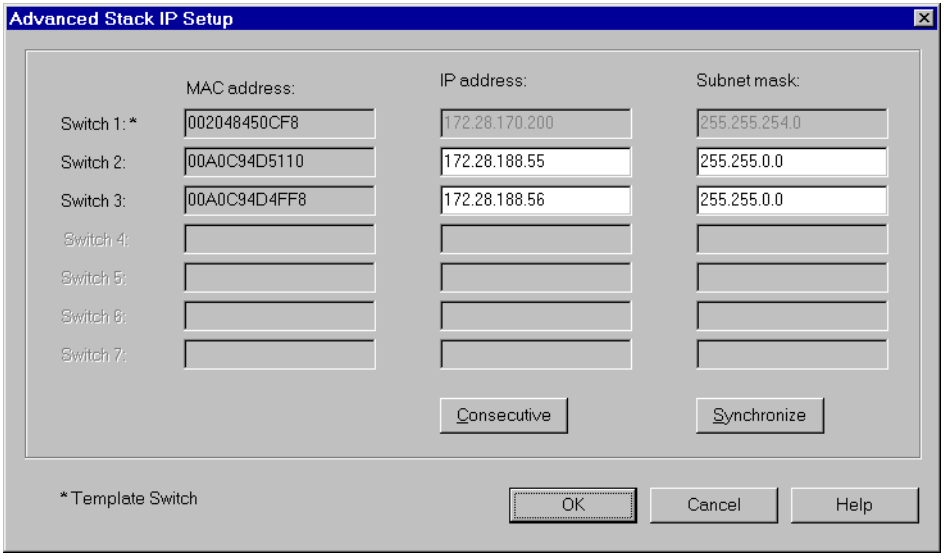


Figure 2.8 - Advanced Stack IP Setup Dialog Box

The Synchronization Wizard completes the installation. The complete stack, including the new switch, then appears in the FORE Stack View window. The Synchronization wizard is described in detail in “Stack Synchronization Manager” on page 5-40.

2.9.5 Managing an Existing Switch or Stack

To manage a switch or stack that has an IP address already assigned:

1. Select `Device>Manage`. The Manage dialog box appears.
2. Type in the switch’s IP Address or MAC address.
3. Select the box if you want to open the switch in a new FORE Stack View window.
4. Click `OK`.

2.9.6 Establishing and Expanding a Stack

If you connect switches that already have IP addresses assigned together via a Matrix Module, you can manage them as a stack. To create or expand an existing stack:

1. Select `Device>Manage`, and the Manage dialog opens.
2. Type in the IP Address or MAC address of one of the switches. All the switches connected via the Matrix Module are displayed in this window, even switches that are already configured as a stack.

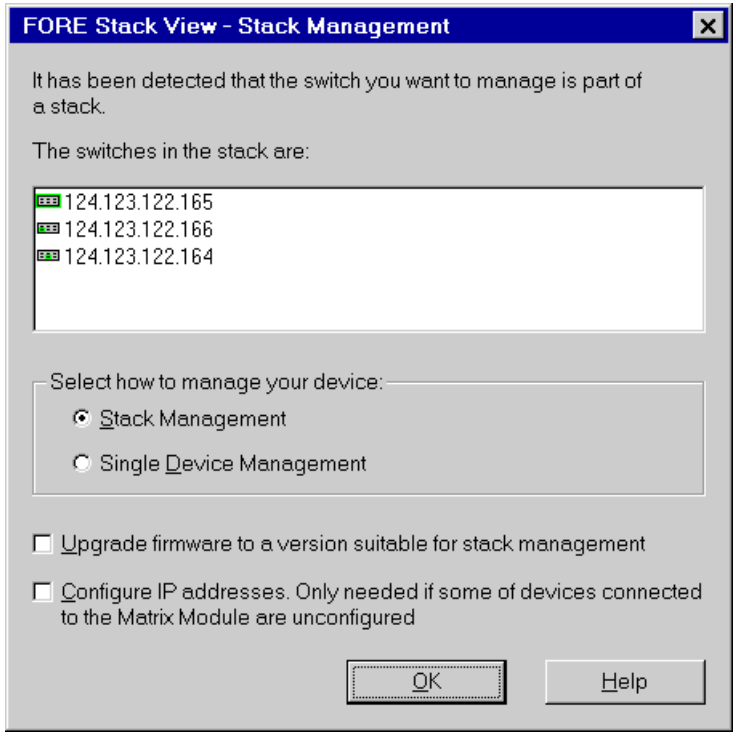


Figure 2.9 - The Manage Dialog Box

3. If the switches don't have compatible software, the `Upgrade` box is checked. If one or more of the switches aren't configured, the Configure `IP address` box is checked.
4. Select `Stack Management`.
5. Select `OK`. The Upgrade Wizard starts automatically if software needs to be upgraded.

2.10 Device Tree

2.10.1 Introduction

The Device Tree displays the separate subnets on your LAN as branches in a tree. This includes a branch that shows all the unconfigured devices on the LAN.

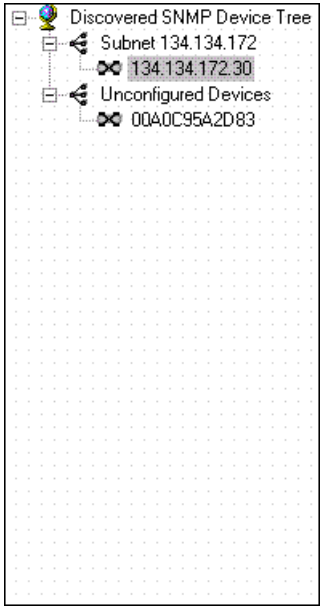


Figure 2.10 - The Device Tree

2.10.2 Identifying Devices

The Device Tree uses several icons to represent the individual devices:

Table 2.2 - Device Icons in the Device Tree

Icons	Device Description
	Recognized as a switch.
	Recognized as a router.
	Recognized as a hub.
	Device contacted, but not recognized.
	Lost contact with device.

2.10.3 Installing and Managing Switches

Double clicking the switch's IP address or MAC address opens existing switches in the FORE Stack View window, or starts the Install Wizard for new switches.

2.10.4 Right Mouse Button Commands

By positioning the mouse pointer in the Device Tree and clicking the right mouse button, the following functions are available:

Table 2.3 - Right Click Command Options in the Device Tree

Is a Device Selected?	Available Functions		Description
No	View	IP Address	Sorts the devices by their IP addresses.
		Name	Sorts the devices by their DNS names.
	Add Device		If a device has not been auto-detected then you can add it to the tree. You need to know its IP address.
	Find		Locates a specific device by searching for its IP address.
	Refresh		Polls the network and redisplays the tree. If a new device has been connected, it will appear after a refresh.
Yes	Launch With		Opens the switch in FORE Stack View.
	Delete		Removes a device from the Device Tree.
	Edit		Change the name, community settings (read and write) and polling rate of the device.
	RMON	Statistics	Provides subnet management statistics.
		History	Lists monitored traffic on a subnet.
		Alarms	Enables activity alarms to be set.
		Logs	Sets events defined by Log, Trap or Log and Trap.

2.11 Device View (Main Display)

2.11.1 Switch Contacted

When FORE Stack View contacts the switch or stack, the front (interface side) of the switch or stack is displayed.

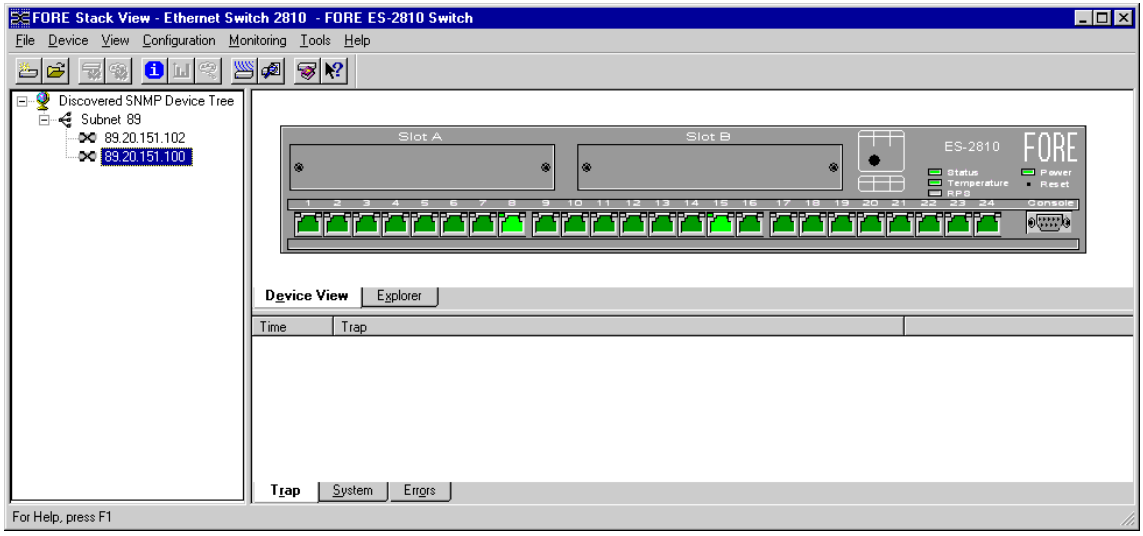


Figure 2.11 - Switch Display in FORE Stack View

This view provides a real-time view of the switch, or stack and ports, which behaves in the same way as the physical switch. For example, the LEDs change color according to the state of the switch / stack. You can fully manage the switch or stack using this display.

2.11.2 Mouse Actions

Using a mouse makes it easier to operate FORE Stack View and saves you time:

Table 2.4 - Mouse Actions in FORE Stack View

Mouse action	Information
Right-click switch	Shows the switch-related menus for configuration and monitoring.
Right-click stack border	Shows the stack-related menus for configuration and monitoring.
Right-click a port	Shows the port-related menus for configuration and monitoring.
Double left-click switch	Opens the Device Setup menu.
Double left-click a port	Opens that port's Setup menu.

2.11.3 Right Mouse Button Commands for a Single Switch

Right click a single switch and FORE Stack View offers:

Table 2.5 - Right Click Command Options for a Single Switch

Functions	Description
Device Setup	Displays comprehensive information about the switch's overall setup.
VLAN Setup	Provides an overview of existing VLANs and the opportunity to add new ones or change existing ones.
Device Information	Informs you about the type of switch, its location, who is responsible for it and the amount of time passed since the switch was restarted.
Port Overview	Gives detailed monitoring information for each port.
Device Activity	Displays, in a graph format, information about the activity on the ports.
VLAN	Displays monitoring information and the status of the VLAN links.
Device	Reboots the switch and provides information about the firmware in the switch. Also enables the switch's firmware to be upgraded.
Configuration	Ensures the switch's configuration is safe by saving it to the flash memory, by backing up to disk and by being able to restore it again should it be lost. If necessary, the switch can be returned to the factory default configuration.
Monitoring	Provides comprehensive details for Spanning Tree statistics and RMON facilities, as well as Hardware information and an Access Overview.

2.11.4 Right Mouse Button Commands for a Stack Border

When managing a stack of switches, right click the stack border to access the functions described in Table 2.6.

Table 2.6 - Right Click Command Options for Stack Borders

Functions	Description
Stack Setup	Displays comprehensive information about the switch's overall setup.
VLAN / Routing Setup	Provides an overview of existing VLANs and the opportunity to add new ones or change existing ones.
IP Filtering Setup	Defines user groups and filters the packets sent to them.
Stack Health Monitor	Provides the IP addresses for all the switches in the stack, the type of switch and whether they are responding to ping.
IntraStack Traffic	Gives information about the traffic through the Matrix Module.
System Information	Gives the name and location of the stack, together with a contact name and the length of time the stack has been running.
Stack Activity	Displays as graphs monitoring information of traffic on the ports in the stack.
Port Overview	Provides port performance, packet distribution and spanning tree information for all the ports in the stack.
Device	Enables you to reboot the stack and provides information about the firmware in the switches.
Configuration	Ensures the stack's configuration is safe by saving it to the flash memory, by backing up to disk and by being able to restore it again should it be lost. If necessary, the stack can be returned to the factory default configuration.
Monitoring	Provides Hardware information about the separate switches in the stacks and the access rights to the devices on the LAN.
Tools	Gives access to the Synchronization Manage, the Switch Position Organizer and Color Code Matrix Ports function.

2.11.5 Right Mouse Button Commands for a Switch in a Stack

When managing a stack of switches, right click a switch to access the functions described in Table 2.7.

Table 2.7 - Right Click Command Options for Switches

Function	Description
IP and Name Setup	Displays the switch's IP address and Subnet mask.
Device Activity	Displays, in a graph format, information about the activity on the ports in the switch selected.
Spanning Tree	Provides statistics about the Spanning Tree on the selected switch.
VLAN	Displays monitoring information and the status of the VLAN links.
Device	Restarts the switch and provides information about the firmware in the switch.
Configuration	Ensures the switch's configuration is safe by saving it to the flash memory.
Monitoring	Displays, as a graph, the activity on all the ports in the switch and RMON facilities.

2.11.6 Right Mouse Button Commands for a Port

Right click a single port to access the functions described in Table 2.8.

Table 2.8 - Right Click Command Options for Ports

Functions	Description
Port Setup	Displays the port status, the speed and duplex settings, and spanning tree settings.
Add Port to VLAN	Adds the port to a VLAN.
Port Details	Displays comprehensive performance, distribution and spanning tree details.
Port Activity	Displays, as a graph, the activity on the port.
VLAN Port Monitoring	Provides details about the MAC and IP addresses on the VLANs.
RMON Statistics	Provides RMON statistics for the selected port.

2.11.7 Color Coding

The switch and ports are displayed in different colors, as described in Table 2.9.

Table 2.9 - Switch and Port Display Colors

Object	Color	Means
Switch Body	Gray	The switch is operational (the software is loaded and running) and it can be contacted by FORE Stack View via the network.
	Dark blue	That switch is selected, and various device-specific parameters can be changed using the right-mouse button.
Ports	Dark green	Port enabled, but no plug connected.
	Light green	Port enabled and plug connected.
	Brown	Port disabled by management or a hardware error.
	Dark blue	That port is selected, and various port-specific parameters can be changed using the right-mouse button.
	Purple	Port mirroring is enabled here.
Stack border	Dark blue	The stack is selected, and various stack-specific parameters can be changed using the right-mouse button.
Everything; switches, ports and stack border	Light blue	FORE Stack View has lost contact with the devices (for example, the switch or your PC is disconnected from the LAN).

2.12 Explorer

2.12.1 FORE Stack View Explorer

The Explorer within FORE Stack View displays management information, for example VLANs on this switch and other switches.

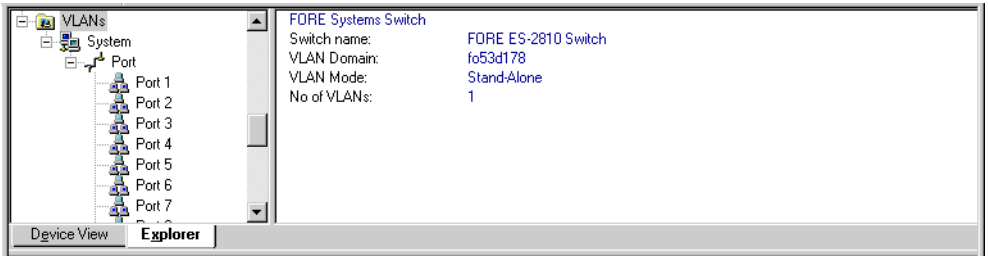


Figure 2.12 - The FORE Stack View Explorer

If a switch is disabled or not operational, it is displayed with a red cross through it.

General management information for the switch is accessed from the Monitoring menu.

2.13 Diagnostics Window

2.13.1 FORE Stack View Diagnostics

The Diagnostics window helps you troubleshoot the switch / stack to get it working properly in case of problems.

The Diagnostics window lists any problems detected by the switch / stack and notes the level of the problem (fatal error, error or note) and the port on which the error occurred. Messages are automatically cleared from the list when the problem no longer exists

2.13.2 Right Mouse Button Commands

Right click a message and FORE Stack View offers:

Table 2.10 - Right Click Command Options in Diagnostics Window

Functions	Description
Details	Displays a diagnostic details window that describes the problem and gives a possible solution.
Refresh	Reloads and updates all the diagnostic information.
Clear	Clears all the messages displayed.
Use Color Coding	Displays the messages in different colors, depending on their severity.

2.13.3 Diagnostic Details Window

The Diagnostic details dialog box, shown in Figure 2.13, provides comprehensive details of the error.

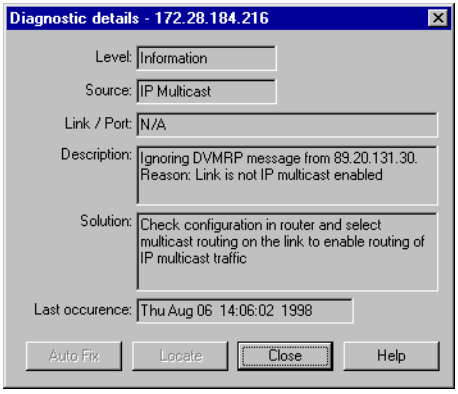


Figure 2.13 - Diagnostic Details Dialog Box

2.14 Trap Window

2.14.1 Traps window

The Traps window displays all traps generated by the switch.

2.14.2 Color Coding

Traps are generated by the switch for many events, both normal and errors. Traps displayed in FORE Stack View are color coded according to the severity of the trap.

2.14.3 Right Mouse Button Commands

Right click a message to access the functions described in Table 2.11.

Table 2.11 - Right Click Command Options in Trap Window

Functions	Description
Refresh	Reloads and updates all the information in this window.
Clear	Clears all the messages displayed.
Properties	Enables color coding to be switched on and off and define maximum number of messages displayed.

2.15 System Window

2.15.1 System Window

The System window contains a log of all the major switch events with date and times (for example, return to factory default, filter entry settings, modules inserted in slots).

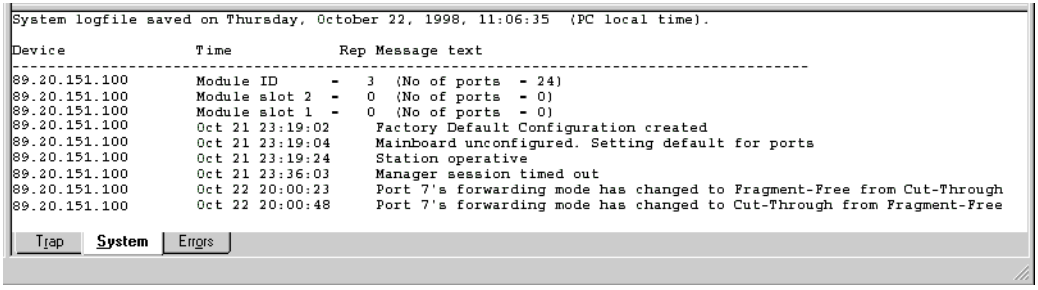


Figure 2.13 - The System Window

2.15.2 Right Mouse Button Commands

Right click a message to access the functions described in Table 2.12.

Table 2.12 - Right Click Command Options in System Window

Functions	Description
Refresh	Reloads and updates all the information in this window.
Clear	Clears all the messages displayed.
Pause	Pauses the normal updating of information in this window.

2.16 Errors Window

2.16.1 Errors Window

The Errors window, shown in Figure 2.14, is a log of all error messages generated by the switch.

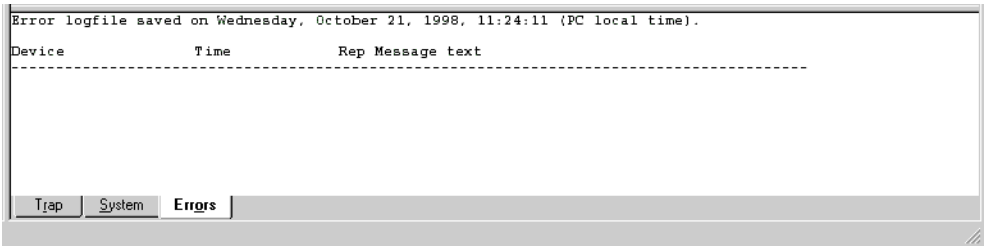


Figure 2.14 - The Error Window

2.16.2 Right Mouse Button Commands

Right click a message to access the functions described in Table 2.13.

Table 2.13 - Right Click Command Options in Error Window

Functions	Description
Refresh	Reloads and updates all the information in this window.
Clear	Clears all the messages displayed.
Pause	Pauses the normal updating of information in this window.

CHAPTER 3 Standard Configuration

3.1 In This Chapter

This chapter covers the topics described in Table 3.1.

Table 3.1 - Topics Discussed in this Chapter

Topic	See Page
Changing the Setup of the Switch or Stack	page 3-2
Changing the Setup of the Port	page 3-27

Chapter 4 contains instructions on how to configure VLANs.

3.2 Changing the Setup of the Switch or Stack

3.2.1 Improving Switch Security

To restrict the use of the switch or stack, you can:

- Change the administrator password for local management.
- Change the user password for local management.
- Limit access to Local Management via the `Console` port and / or Telnet.
- Specify a time of "no input", after which the connection with Local Management is terminated.
- Change the password for moving files with TFTP.
- Specify use of TFTP.
- Restrict access to include only the stations named on the Authentications list.

3.2.2 Using the Mouse

There are two ways to access the `Device Setup` (for single switches) or `Stack Setup` window:

- Double-click the switch or the stack border.
- Right-click the switch or the stack border.

3.3 System Configuration

3.3.1 Identifying the Switch

To assist with switch identification and administration, you can change certain switch details (name, location and contact person). With a switch or stack in the Device View window:

1. Select `Device Setup` or `Stack Setup`.
2. Click `System`.

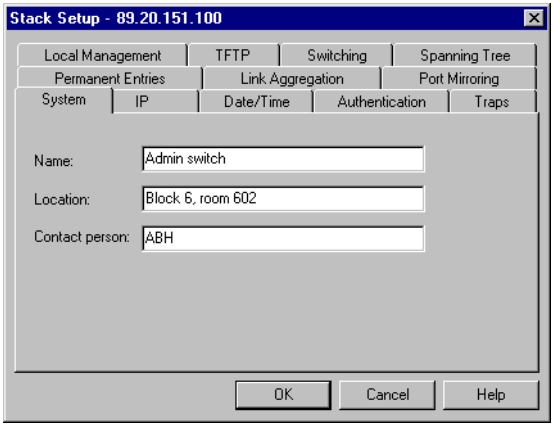


Figure 3.1 - Stack Setup Dialog Box

3. Change the details.
4. Click `OK`.

   These details are used by SNMP management centers.

3.4 Internet Protocol Configuration

3.4.1 Changing IP Details

The IP configuration information is used to contact the switch via IP protocols (TFTP, SNMP, TELNET etc.). To change the main IP address and network mask:

1. Select `Device Setup` or `Stack Setup`.
2. Click `IP`.

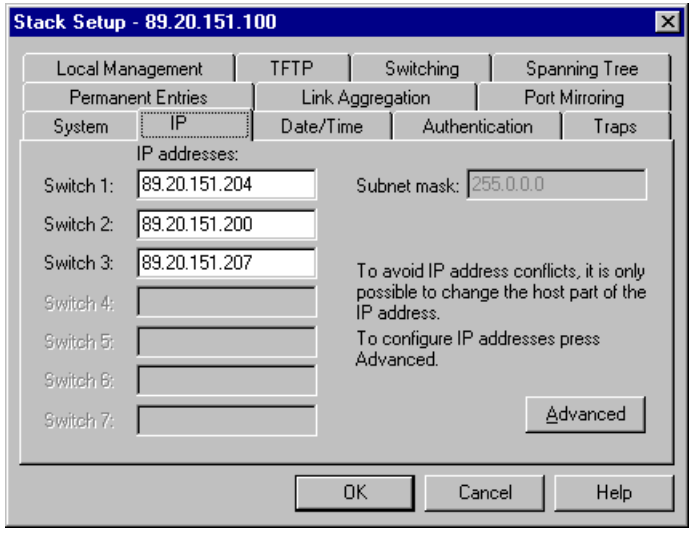


Figure 3.2 - IP Tab of the Stack Setup Dialog Box

3. Change the details.
4. Click `OK`.

3.5 Local Time Configuration

3.5.1 Setting the Date and Clock to Local Time

To change the clock in the switch to your local time:

1. Select `Device Setup` or `Stack Setup`.
2. Click `Date/Time`.

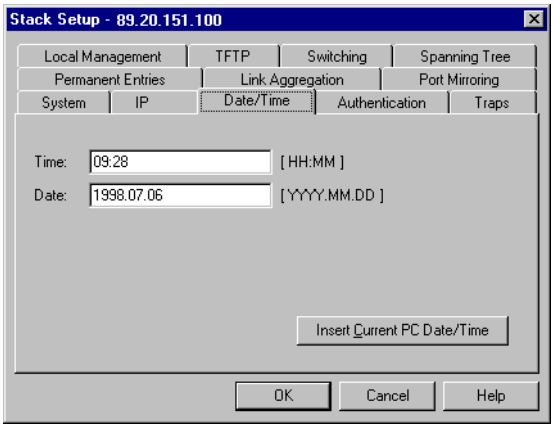


Figure 3.3 - Date / Time Tab of the Stack Setup Dialog

3. Click `Insert Current PC Date/Time` to show the present settings. If this is satisfactory, click `OK`.

NOTE

The clock displays the time at which it is accessed and not the current time.

4. If the time or the date is not satisfactory, click the date and / or time options and type the new time and date.
5. Click `OK`.

3.6 Authentication

3.6.1 Purpose

SNMP is a fully defined, interoperative standard that helps you manage both the switch and the network. To do this you can:

- Specify the names of the hosts to access the SNMP agent on the switch (authentication) by defining the source IP and community
- Specify read-write or read-only for authenticated hosts
- Request a trap to be sent if authentication is violated

If no hosts are defined in the Authentication List, any host can access the SNMP agent in the switch.

3.6.2 Security

The authentications list defines the hosts that can carry out SNMP, TFTP or Telnet management on the switch, have read-write or read-only rights and access to communities. You can:

- Add a new entry to the list
- Delete an entry
- Edit existing entries

3.6.3 Adding a Device

To add a host that is allowed to carry out management on the switch:

1. Select `Device Setup` or `Stack Setup`.
2. Click `Authentications`.

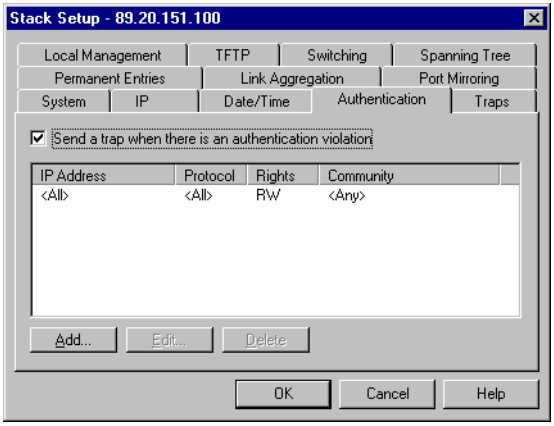


Figure 3.4 - Authentication Tab of the Stack Setup Dialog Box

3. Click `Send trap when authentication violation`.

   A message will be sent to the `Traps` window if unauthorized hosts try to carry out management on the switch.
4. Click `Add`.
5. In `IP address`, type the IP address of the device to manage the switch.

   You can have a maximum of eight addresses in the list. The address 0.0.0.0 indicates that all IP addresses are accepted.
6. Click `Protocol` and select one.
7. Click `Rights` and specify the level of access to the switch
8. For SNMP only, click `Community` and type the SNMP request name accepted by the SNMP agent.

   If no community name is specified, all community names are accepted by the SNMP agent.
9. Click `OK`.

3.7 Traps

3.7.1 Purpose

A trap alerts you of events occurring in the switch. The traps list shows where SNMP traps (generated by the switch) are sent. You can:

- Add a new entry to the list
- Delete an entry
- Edit existing entries

3.7.2 Adding a Trap

NOTE

If there are no entries in the Traps list, then no SNMP traps are sent.

1. Select `Device Setup` or `Stack Setup`.
2. Click `Traps`.

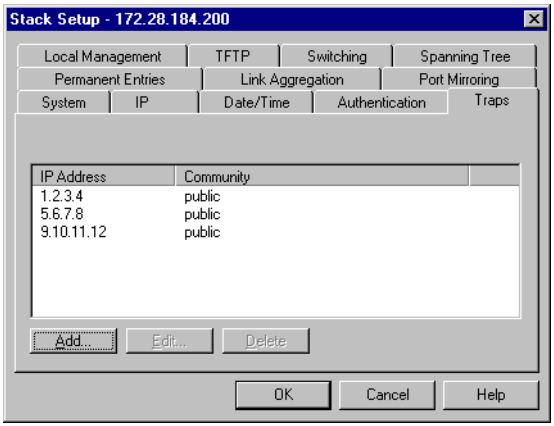


Figure 3.5 - Traps Tab of the Stack Setup Dialog Box

3. Click `Add`.
4. Type the Destination IP address, or click `This PC`.
5. Type the community (SNMP password).
6. Click `OK`.

3.8 Permanent Entries

3.8.1 Purpose

You can permanently allocate a port to a device that does not send out device information. These devices are not removed from the switch's address table, regardless of how long they are quiet. This is useful for connections to printers and other similar devices. You can:

- Add a new entry to the list
- Delete an entry
- Edit existing entries

3.8.2 Adding a Permanent Entry

To add a device to the switch's address table:

1. Select `Device Setup` or `Stack Setup`.
2. Click `Permanent Entries`.

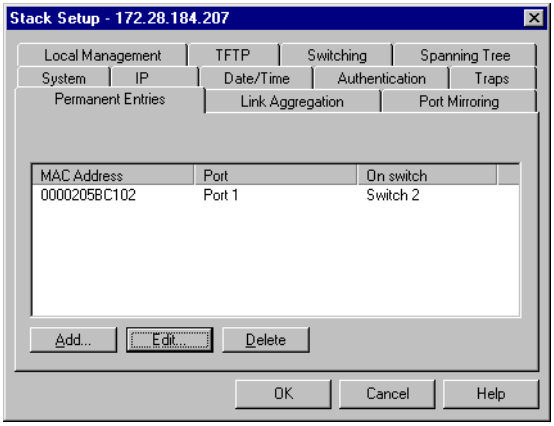


Figure 3.6 - Permanent Entries Tab of the Stack Setup Dialog Box

3. Click `Add`.
4. Type the device's MAC address.
5. Click `Port number` and select one. A permanent entry is only made on the defined port.
6. Click `OK`.

3.9 Link Aggregation

3.9.1 Purpose

You can combines two or four adjacent ports to increase the bandwidth between two switches or stacks. You can add a new entry to the list or delete an entry.

3.9.2 Adding an Aggregate Link

To set up and add an aggregate link:

1. Select `Device Setup` or `Stack Setup`.
2. Click `Link Aggregation`.

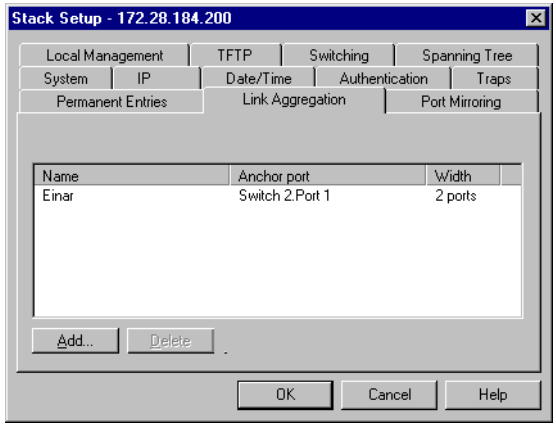


Figure 3.7 - Link Aggregation Tab of the Stack Setup Dialog Box

3. Click `Add`.
4. For a stack, click `Switch` and select one from the list.
5. Click `Aggregation width:` and select `2 Ports` or `4 Ports`.
6. Click `Anchor Port` and select a port.
7. Type a unique name for the link.
8. Click `OK`. For further configuration of a link, for example in a VLAN, use the Anchor Port.

3.10 Port Mirroring

3.10.1 Purpose

The Port Mirroring function allows you to debug or monitor traffic on a specific port by duplicating the traffic and sending it to a specified port. Only one pair of ports can be mirrored per switch. Within Port Mirroring, you can:

- Add a new entry to the list
- Delete an entry
- Edit existing entries

3.10.2 Adding Port Mirroring

To add a mirrored port to a switch:

NOTE

If Port Mirroring is enabled, the source port will be in store-and-forward mode. Therefore, Runts, CRCs, etc. will not be forwarded or mirrored.

1. Select `Device Setup` or `Stack Setup`.
2. Click `Port Mirroring`.

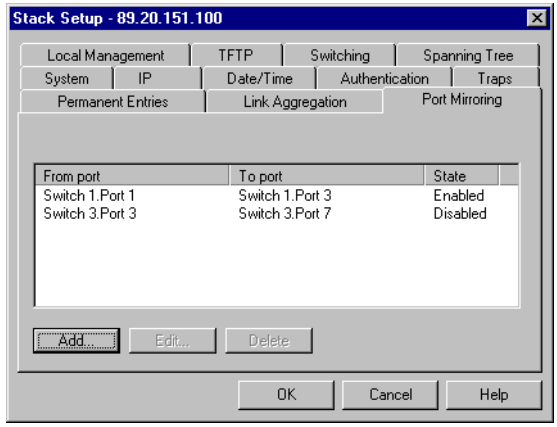


Figure 3.8 - Port Mirroring Tab of the Stack Setup Dialog Box

3. Click `Add`.
4. For a stack, click `Switch` and select one.
5. Click `Reflect from` and select the port that you want.
6. Click `Reflect to` and select the port to where the traffic can be debugged / monitored.
7. Click `OK`.

3.11 Local Management

3.11.1 Changing Password Details

The administrator has read-write access at all levels. The user can read the monitoring screens, but cannot change the configuration, update software or reset the station. To prevent unauthorized personnel changing configurations:

1. Select `Device Setup` or `Stack Setup`.
2. Click `Local Management`.

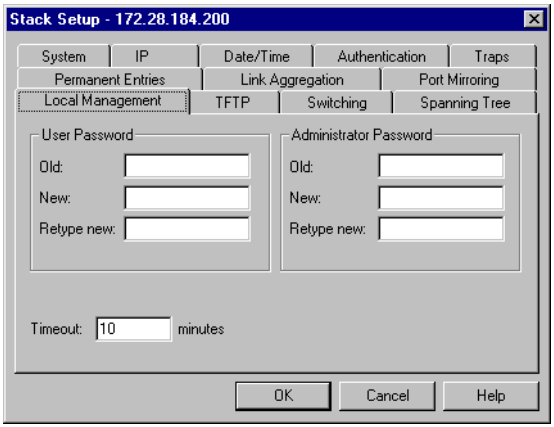


Figure 3.9 - Local Management Tab of the Stack Setup Dialog Box

3. You can change the passwords for the Administrator and User.
4. Type the old password.
5. Type the new password.
6. Retype the new password (in `Retype new`).
7. Click `OK`.

3.11.2 Changing Timeout Details

When there has been no input during the timeout interval, the connection with Local Management is terminated. To change the timeout interval:

1. Select `Configuration>Device Setup`.
2. Click `Local Management`.
3. Type the new time.
4. Click `OK`.

3.12 TFTP

3.12.1 Changing Password Details

To give added security, you can limit the number of staff authorized to transfer TFTP files by changing the TFTP password. To change the password:

1. Select `Device Setup` or `Stack Setup`.
2. Click `TFTP`.
3. Type the old password.
4. Type the new password.
5. Retype the new password (in `Retype new`).
6. Select `OK`.

3.13 Switching

3.13.1 Changing the MAC Address Ageing Time

To change the time a MAC address is kept in the filter before being purged:

1. Select `Device Setup` or `Stack Setup`.
2. Click `Switching`.

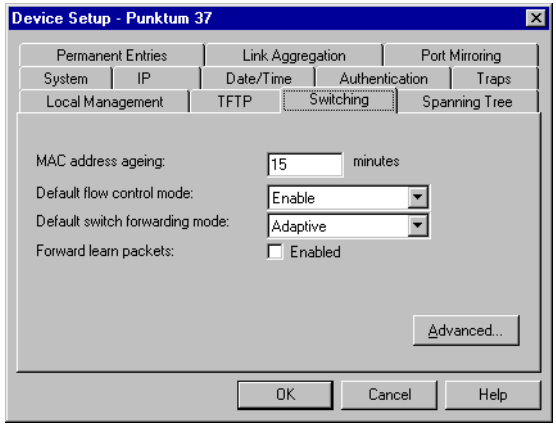


Figure 3.10 - Switching Tab of the Device Setup Dialog Box

3. Click `MAC Address Ageing`.
4. Type the required number of minutes.
5. Click `OK`.

3.13.2 Changing the Flow Control

Flow control prevents the loss of frames during busy periods. Note that the individual port settings overrule the default setting. To change the default flow mechanism on all ports:

1. Select `Device Setup` or `Stack Setup`.
2. Click `Switching`.
3. Click `Default Flow Control`.
4. Click `Enabled` or `Disabled`.
5. Click `OK`.

3.13.3 Changing the Default Forwarding Mode

To change the forwarding mode to be used on all ports:

1. Select `Device Setup` or `Stack Setup`.
2. Click `Switching`.
3. Click `Default Switch Forwarding Mode`.
4. Click the default forwarding mode you want.
5. Click `OK`.

3.13.4 Enable Forward Learn Packets Mode

When this mode is enabled, all packets are forwarded. However, if there is not enough memory in the switch, due to heavy load, the packet is discarded. When this mode is disabled, only "IPX Get server" request packets are forwarded. To enable or disable this mode:

1. Select `Device Setup` or `Stack Setup`.
2. Click `Switching`.
3. Check the box to enable this mode.
4. Click `OK`.

3.14 Adaptive Forwarding Mode

3.14.1 Purpose

You can:

- Change the Sample Time
- Define the minimum and maximum errors acceptable before changing the forwarding mode

While CRC errors and runts are the most likely parameters to cause the switching mode to change, they are not the only ones.

3.14.2 Changing the Time to Measure Errors

The sample time should be the shortest time needed to detect errors. If the sample time is too great, there may be too many errors before the forwarding mode changes. To change the time the switch retains error counters:

1. Select `Device Setup` or `Stack Setup`.
2. Click `Switching`.
3. Click `Advanced`.

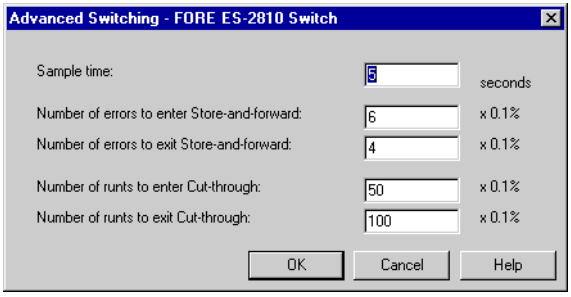


Figure 3.11 - Advanced Switching Dialog Box

4. Click `Sample Time`.
5. Type the required number of seconds.
6. Click `OK`.

3.14.3 Changing Number of Errors Before Adaptive Forwarding Mode Operates

Adaptive forwarding changes the forwarding mode depending on the upper and lower limits of specific error types. To change the number of upper and lower limits:

1. Select `Device Setup` or `Stack Setup`.
2. Click `Switching`.
3. Click `Advanced`.
4. Click the required parameter.
5. Type the percentage of errors or runts.
6. Click `OK`.

3.15 Spanning Tree

3.15.1 Purpose

You can change the:

- Priority given to the switch
- Maximum length of time information is retained by the switch
- Time between transmitted Configuration BPDUs
- Time the switch spends in the Listening and Learning states

3.15.2 Warning When Using VLANs

It is important to be aware of problems that may arise when using Spanning Tree and VLANs. The Spanning Tree can use alternative paths (such as different ports) to get messages to their destination.

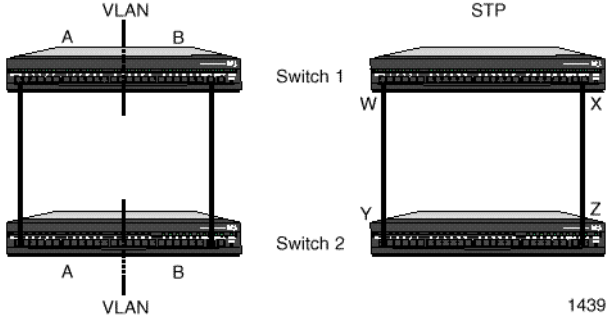


Figure 3.12 - Spanning Tree Blocking to Prevent Loops

The diagram above, shows two switches. On the left, we see the two switches connected and the ports are grouped in two VLANs: A and B. On the right, we have enabled STP; STP blocks the path between X and Z (to avoid looping) and, therefore, destroys the VLAN setup (because VLAN B needs these ports to receive messages).

3.15.3 Why Change These From Their Defaults?

The switch is delivered with Spanning Tree default values set to those recommended by the IEEE 802.1d standard. These values are conservative worst-case estimates for LANs consisting of a large number of switches. Therefore, changing these default values may improve the performance of your network.

3.15.4 Changing the Spanning Tree Priority

The higher the value, the lower the chance of the switch being used as the root bridge. To change the priority value:

1. Select `Device Setup` or `Stack Setup`.
2. Click `Spanning Tree`.

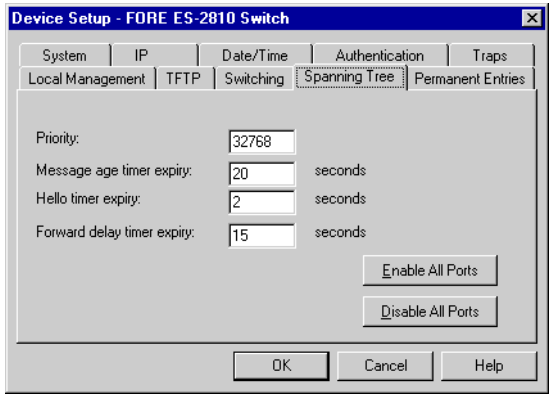


Figure 3.13 - Spanning Tree Tab of Stack Setup Dialog Box

3. Click `Priority`.
4. Type the required value.
5. Click `OK`.

3.15.5 Changing the Message Age Expiry Time

To change the maximum time between protocol information being received and discarded:

1. Select `Device Setup` or `Stack Setup`.
2. Click `Spanning Tree`.
3. Click `Message Age Timer Expiry`.
4. Type the required number of seconds.
5. Click `OK`.

3.15.6 Changing the Hello Expiry Time

To change the time between transmissions of configuration BPDUs from a switch that is, or attempting to become, the root:

1. Select `Device Setup` or `Stack Setup`.
2. Click `Spanning Tree`.
3. Click `Hello Timer Expiry`.
4. Type the required number of seconds.
5. Click `OK`.

3.15.7 Changing the Forward Delay Expiry Time

To change the time between port states while the bridge attempts to become the root:

1. Select `Device Setup` or `Stack Setup`.
2. Click `Spanning Tree`.
3. Click `Forward Delay Timer Expiry`.
4. Type the required number of seconds.
5. Click `OK`.

3.15.8 Changing the State of the Ports

To specify that all ports are using Spanning Tree Protocol:

1. Select `Device Setup` or `Stack Setup`.
2. Click `Spanning Tree`.
3. Click `Enable All Ports`.

   The ports are able to resolve problematic network loops using STP.
4. Click `OK`.

3.16 Changing the Setup of the Port

3.16.1 Purpose

You can configure the port to operate in different ways, according to your network's requirements:

- Change the port state
- Select the auto-negotiation mode
- Change each port to half or full duplex

  (If auto-negotiation is not enabled)
- Specify the speed of the port

  (If auto-negotiation is not enabled)
- Change the forwarding mode of the port
- Change the flow control setting of the port
- Specify the spanning tree

3.16.2 Using the Mouse

There are two ways to access the Port Setup window:

- Double-click the port
- Right-click on the port, and click `Port Setup`

3.17 General Changes

3.17.1 Renaming a Port

To give a port a new name, for example, its use or the user(s) connected:

1. Click the port you want to rename.
2. Select `Port Setup`.
3. Click `General`.

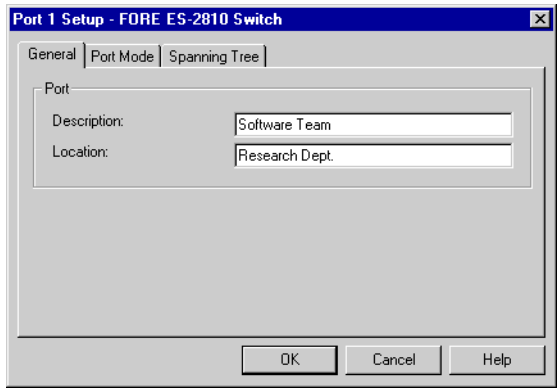


Figure 3.14 - General Tab of Port Setup Dialog Box

4. In `Description`, type the new name.
5. Click `OK`.

3.17.2 Location for a Port

To specify the location (for example, an office number or department) of the device attached to a port:

1. Click the port you want to give a home to.
2. Select `Port Setup`.
3. Click `General`.
4. In `Location`, type where the device is.
5. Click `OK`.

3.18 Port Mode

3.18.1 Disabling the Port

If you disable the port, the devices attached to it cannot use the switch. The MAC address of those devices are removed from the switch's address table. If those addresses are defined as permanent entries, they are not purged but are unable to use the switch. To disable the port:

1. Click the port you want to disable.
2. Select `Port Setup`.
3. Click `Port Mode`.

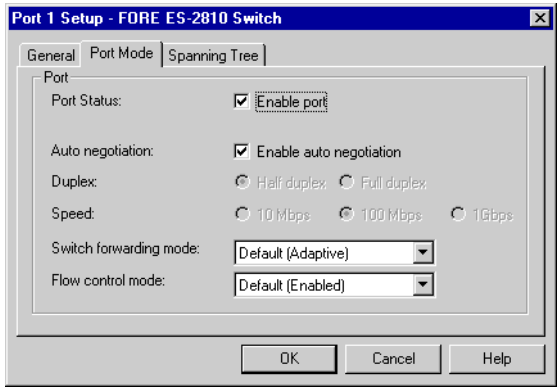


Figure 3.15 - Port Mode Tab of Port Setup Dialog Box

4. Click `Enable Port`.

   If there is a check mark in the box, the port is operational. If the box is empty, the port is disabled.
5. Click `OK`.

3.18.2 Disabling Auto-negotiation

To disable auto-negotiation, and reset the speed to the values specified in Speed:

1. Click the port you want to disable auto-negotiation.
2. Select Port Setup.
3. Click Port Mode.
4. Click Enable Auto-negotiation.

   If there is a check mark in the box, the port automatically detects the line-speed and duplex setting. If the box is empty, auto-negotiation is disabled and the port uses the values specified in Duplex and Speed.
5. Click OK.

3.18.3 Changing Duplex Mode

To change the port's duplex mode (when auto-negotiation is disabled):

1. Click the port you want to change.
2. Select Port Setup.
3. Click Port Mode.
4. Click Half Duplex or Full Duplex.

   Half allows either transmission or receipt of the data and Full allows both transmission and receipt of the data.
5. Click OK.

3.18.4 Changing the Port Speed

To change the speed a port accepts data (when auto-negotiation is disabled):

1. Click the port you want to change.
2. Select Port Setup.
3. Click Port Mode.
4. Click Speed 10 or Speed 100.

   10 limits data entering to 10Mbps and 100 allows data speeds up to 100Mbps.
5. Click OK.

3.18.5 Changing the Forwarding Mode on a Port

To change the forwarding mode to be used on a port:

1. Click the port you want to change.
2. Select `Port Setup`.
3. Click `Port Mode`.
4. In `Switch Forwarding Mode`, click the forwarding mode you want.

   `Default` uses the same forwarding mode as specified in `Device Setup`.
5. Click `OK`.

3.18.6 Changing the Flow Control on a Port

Flow control prevents the loss of frames during busy periods. To change the flow mechanism on a port:

This feature is over-ridden by disabling the flow control setting in `Device Setup>Switching`.

1. Click the port you want to change.
2. Select `Port Setup`.
3. Click `Port Mode`.
4. In `Flow Control`, click the flow control you want.

   `Default` uses the same flow control as specified in `Device Setup`.
5. Click `OK`.

3.19 Port Specific Spanning Tree

3.19.1 Purpose

You can:

- View the Spanning Tree setups for the port
- Specify whether STP (Spanning Tree Protocol) is enabled on the port
- Define which ports are going to be used most frequently

3.19.2 Changing the State of a Port

To specify that a port is using STP:

1. Click the port you want to change.
2. Select `Port Setup`.
3. Click `Spanning Tree`.

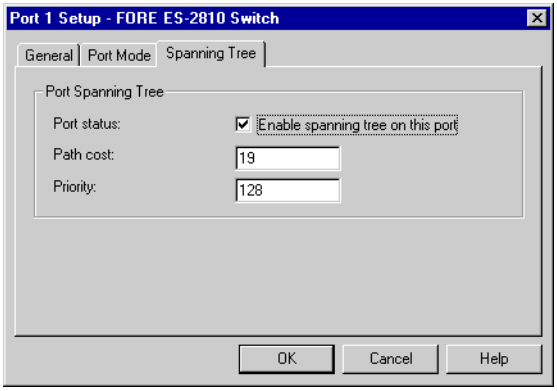


Figure 3.16 - Spanning Tree Tab of the Port Setup Dialog Box

4. Click `Enable spanning tree on this port`.

   If there is a check mark in the box, the port is used in STP. If the box is empty, the port is not used in STP.
5. Click `OK`.

3.19.3 Changing the Cost of the Path

The higher the cost, the lower the chance of this port being used for forwarding traffic, if there is an alternative route. When possible, give a port a low cost if it is connected to a faster network segment. To change the overall cost of the path between a port and the segment:

1. Click the port you want to change.
2. Select `Port Setup`.
3. Click `Spanning Tree`.
4. Select the `Port status` box.
5. In `Path cost`, type the required value.
6. Click `OK`.

3.19.4 Changing Priority of the Port in the Spanning Tree

The higher the value, the lower the chance of this port being used as the designated or root port. To change the priority value:

1. Click the port you want to change.
2. Select `Port Setup`.
3. Click `Spanning Tree`.
4. Select the `Port status` box.
5. In `Priority`, type the required value.

   If there are two ports with the same value, the port with the lowest port number is chosen.
6. Click `OK`.

CHAPTER 4 Advanced Configuration

4.1 In this Chapter

In this chapter you will learn how to configure the ES-2810's Virtual LAN (VLAN) features.

You can create logical network groups (VLANs) by segmenting the switch; for example, according to the subnetting scheme within your network. Each VLAN is an isolated group and the switch only forwards traffic between members of the same group. Communication between groups can be implemented using routers.

4.2 VLANs (Virtual LANs)

4.2.1 Purpose

You can use VLANs to:

- Create up to 128 separate user groups
- Limit broadcast and multicast traffic
- Increase security by limiting communication between groups
- Allocate network resources (such as servers) to groups

For a more comprehensive explanation of the VLAN concept, refer to the online help.

4.2.2 Warning When Using the Spanning Tree Protocol

It is important to be aware of problems that may arise when using Spanning Tree and VLANs. The Spanning Tree Protocol can use alternative paths (such as different ports) to get messages to their destination. VLANs specify which ports can receive messages (see "Spanning Tree" on page 3-23).

WARNING!

When using the Spanning Tree facility, use only one VLAN. If you use two or more VLANs, unexpected changes in your network topology may occur.

4.2.3 Policy-based VLANs

The switch or stack uses "Policy-based VLANs". This means that the devices attached to the switch / stack can be grouped by any combination of MAC address, IP address, IP net and port number; therefore, devices can belong to one or more VLANs.

4.2.4 Policy Hierarchy

To avoid conflicts between two VLANs, a strict priority of the policies is used:

1. MAC address
2. IP address and IP net
3. Port

WARNING!

This means that a station learned by a MAC rule is not learned by an IP or Port rule, and a station learned by an IP rule is not learned by a Port rule. Only stations that are not learned by MAC or IP rules are learned by a Port rule.

IP policies can be used only when IP learning is enabled on the respective ports.

4.2.5 Adding a VLAN

The task of adding VLANs is simplified by using the VLAN Wizard. VLANs are not switch specific when managing a stack. Therefore, right-click the stack border to access VLAN Setup. To add a VLAN:

1. Select `VLAN Setup`.

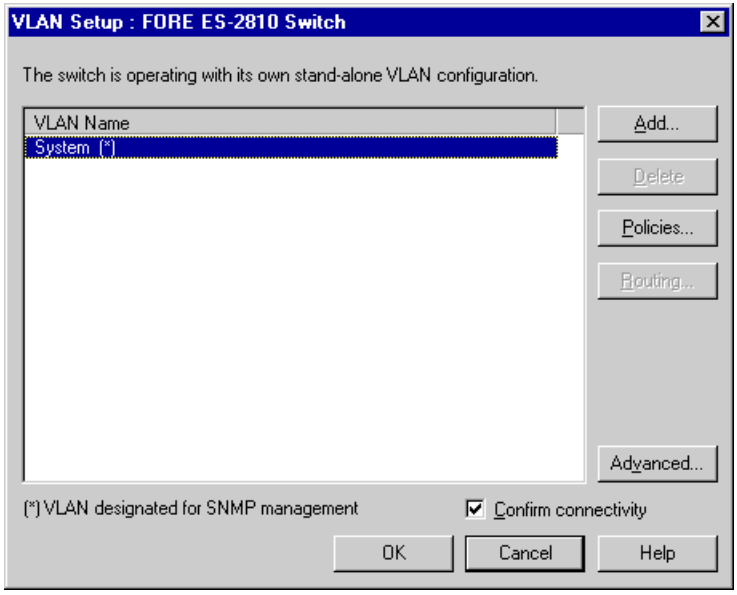


Figure 4.1 - VLAN Setup Dialog Box

2. Click Add, and follow the instructions in the Wizard windows.

Table 4.1 - Information Required for Policies

Policy	Information required
Switch Ports	Port numbers
IP Subnet	IP Subnet and Mask
Mixed policy	IP Subnet and Mask, Port numbers, MAC address and / or IP address

4.2.6 Deleting a VLAN

To delete a VLAN:

1. Select `VLAN Setup`.
2. Click the name of the VLAN you want to delete. (Note: you cannot delete a VLAN if it is the `[Designated Management VLAN]`. To do this, click another VLAN, click `Properties` and then click `Use this VLAN for SNMP management`. You can now delete the first VLAN.)
3. Click `Delete`.

4.2.7 Changing VLAN Mode

To change the mode of operation of a VLAN:

1. Select `VLAN Setup`.
2. Click `Advanced`. The VLAN mode is shown.

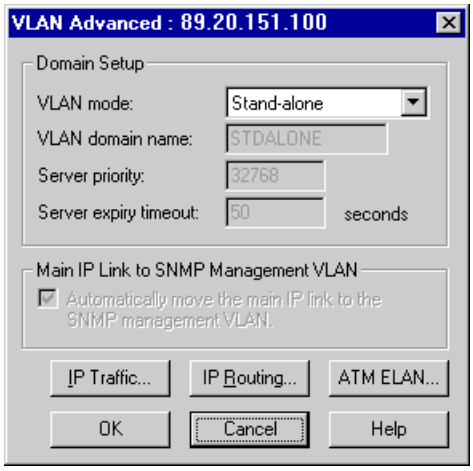


Figure 4.2 - VLAN Advanced Dialog Box

3. Click the VLAN mode to see the full range of choices.

Table 4.2 - VLAN Mode Options

VLAN Mode	Description
Stand-alone	***For single switches:*** There is no exchange of information with VLANs on other switches; each switch is its own domain (STDALONE).
	For switches in a stack: There is an exchange of information using VLANs between the switches in the stack; these switches are in their own domain (STDALONE).
Distributed	A domain is a collection of switches and can contain up to 128 VLANs. If you select distributed, each switch will be able to communicate with all the others in this domain.

4. Click the new mode and make sure the rest of the details are correct.
5. Click OK.

   Your switch may turn blue (for a few seconds) while the network stability returns; this is normal.

4.2.8 Ports with IP Learning

IP learning must be enabled when using IP policies. (IP learning is enabled on all ports by default.) If you want to change the settings for individual ports, for example if you are using protocols other that IP protocols and don't want these stations to be learned using IP rules, you should:

1. Select `VLAN Setup`.
2. Click `Advanced`.
3. Click `IP Traffic`. In the IP Traffic dialog box you can specify which ports support IP learning.

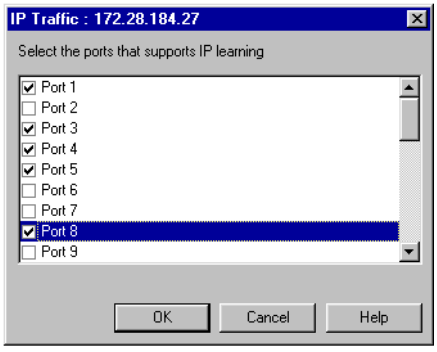


Figure 4.3 - IP Traffic Dialog Box

4. Click `OK`.

4.3 IGMP Pruning

4.3.1 Warning when Using Pruning

It is important to be aware of problems that may arise when using IGMP pruning and IP Multicast addresses.

WARNING!

When using the IGMP pruning, IP multicast packets not based on IGMP are discarded.

4.3.2 Enabling IGMP Pruning

IGMP pruning implements a system where only the necessary amount of IP multicast packets are bridged. To enable IGMP pruning:

1. Select `VLAN Setup`.
2. Click `Advanced>IP Routing>IGMP`.
3. Check `Enabled`.
4. In `Pruning timeout`, type the new value.
5. Click `OK`.

4.4 ATM ELANs

4.4.1 Introduction

This facility enables you to map VLANs defined on the Ethernet switch to ELANs on an ATM switch.

4.4.2 Hardware Requirements

The ES-2810 Ethernet switch must be connected to an FSM-8/TX module installed in an ES-3810 switch. The ES-3810 also must have an ATM Uplink module installed, which is connected to the ATM switch. The cables between the ES-2810 and ES-3810 must be cross-cables. Multiple links made between the switches must not cross between the VLANs. For example, a cable connecting a port in VLAN_1 must not be connected to a port in VLAN_2 in the other switch.

4.4.3 Configuration

The VLANs in the Ethernet switch must be port-based, and only one VLAN per port may be defined. When multiple links are set within a VLAN, Spanning Tree Protocol (STP) must be enabled in both switches to prevent loops being created.

VLANs using MAC address, IP address and IP Net policies must be deleted before enabling ATM ELAN.

4.4.4 Enabling ATM ELAN

This must be enabled when mapping VLANs in an Ethernet switch to ELANs in an ATM switch. To enable this:

1. Select `VLAN/Routing Setup.`
2. Click `Advanced>ATM ELAN.`
3. Check `Enable.`
4. Click `OK`.

4.4.5 Monitoring STP Groups

To monitor all spanning tree groups, other than those on the Management VLAN, establish a telnet session:

1. Use the procedure described in “TFTP” on page 3-17 to start a telnet session
2. Click `Monitoring>STP.`
3. Select either `Port` or `Bridge.`
4. Select a VLAN from the list. All the Port or Bridge details are displayed.

CHAPTER 5 Managing the Switch

5.1 In this Chapter

This chapter covers the topics described in Table 5.1.

Table 5.1 - Topics Discussed in this Chapter

5.2 Management Using FORE Stack View

5.2.1 Why use FORE Stack View?

FORE Stack View allows you to:

- Configure system, switching, IP, spanning tree, authentication, and trap parameters for the switch.
- Configure port-related parameters.
- View traps, logs, traces, and reports generated by the switch.
- Monitor port activity.
- Monitor port faults.
- Monitor switch activity.
- Monitor VLANs.

5.3 Information About the Switch

5.3.1 Identifying the Switch

Use the following procedure to see the name of the switch, the IP address, the administrator's name and how long the switch has been running:

1. Select `Device Information`.

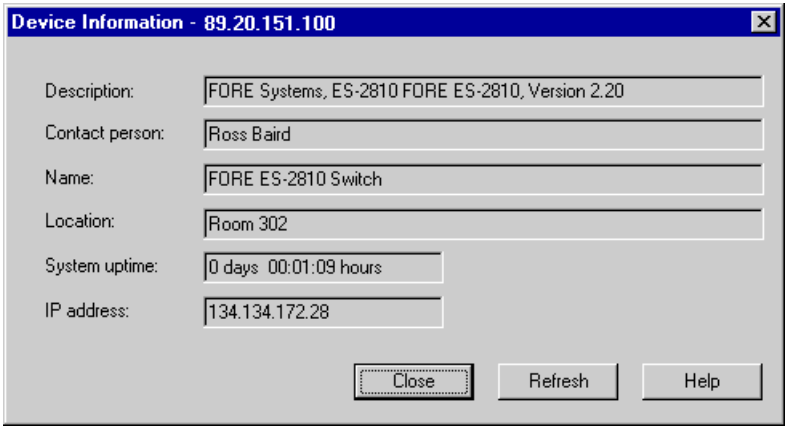


Figure 5.1 - Device Information Dialog Box

2. To update the information, click `Refresh`.

5.3.2 Hardware Details

Use the following procedure to see the MAC address, hardware version and memory size:

1. Click `Monitoring>Hardware Information`.

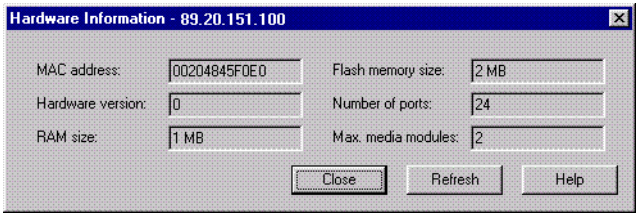


Figure 5.2 - Hardware Information Dialog Box

2. To update the information, click `Refresh`.

5.4 Monitoring the Switch's Performance

5.4.1 Monitoring the Total Packet Activity

Use the following procedure to view the total activity of the packets on all the ports:

1. Select `Device Activity>Total Packets`.

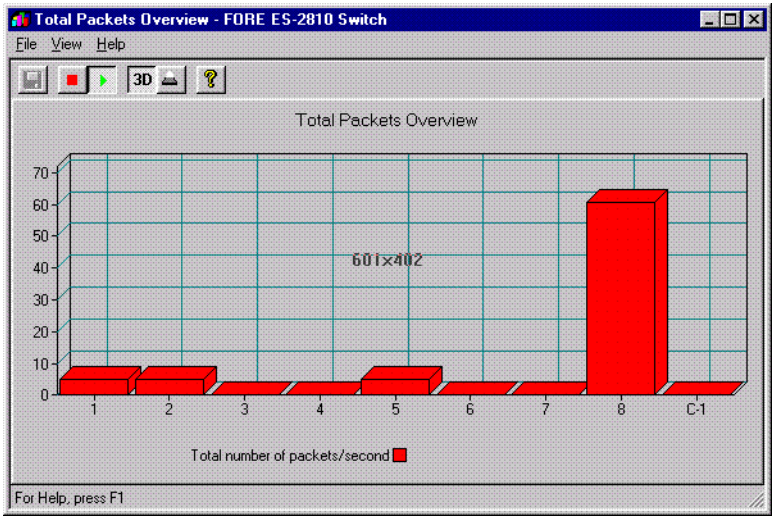


Figure 5.3 - Total Packets View

   Each column represents a port and its activity level.

2. To see the exact value, hold the mouse pointer over a port.
3. Click `View` and change the presentation style: 3D- to 2D-Graph, with or without a peak value indicator and vertical to horizontal bars.

5.4.2 Monitoring the Total Activity of Transmitted Packets

Use the following procedure to view the total activity of the packets being transmitted on all the ports:

1. Select `Device Activity>Tx Packets`.

   Each column represents the activity level on that port.

2. To see the exact value, hold the mouse pointer over a port.
3. Click `View` and change the presentation style: 3D- to 2D-Graph, with or without a peak value indicator and vertical to horizontal bars.

5.4.3 Monitoring the Total Activity of Received Packets

Use the following procedure to view the total activity of the packets being received on all the ports:

1. Select `Device Activity>Rx Packets`.

   Each column represents the activity level on that port.

2. To see the exact value, hold the mouse pointer over a port.
3. Click `View` and change the presentation style: 3D- to 2D-Graph, with or without a peak value indicator and vertical to horizontal bars.

5.4.4 Monitoring the Total Number of Errors

Use the following procedure to view the total error activity of the packets on all the ports:

1. Select `Device Activity>Errors`.

   Each column represents the activity level on that port.

2. To see the exact value, hold the mouse pointer over a port.
3. Click `View` and change the presentation style: 3D- to 2D-Graph, with or without a peak value indicator and vertical to horizontal bars.

5.4.5 Monitoring the Spanning Tree Statistics

To view the spanning tree statistics for the whole switch, select `Spanning Tree Statistics`. The Spanning Tree Statistics dialog box appears, as shown in Figure 5.4.

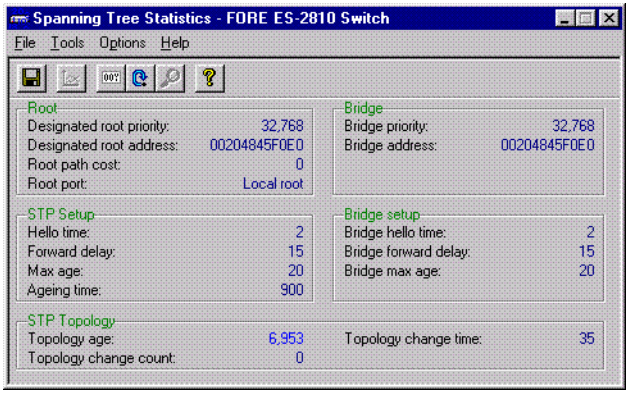
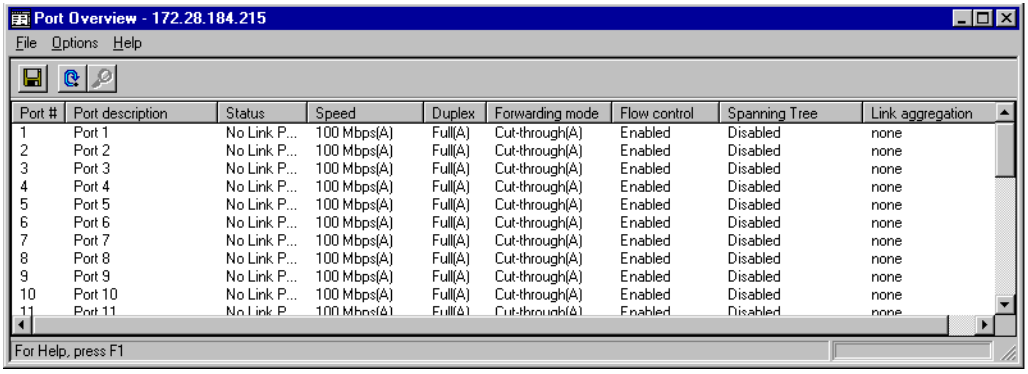


Figure 5.4 - Spanning Tree Statistics Dialog Box

5.4.6 Overview of All the Ports

Use the following procedure to view the setups of all the ports on the switch:

1. Select `Port Overview`.



Port #	Port description	Status	Speed	Duplex	Forwarding mode	Flow control	Spanning Tree	Link aggregation
1	Port 1	No Link P...	100 Mbps(A)	Full(A)	Cut-through(A)	Enabled	Disabled	none
2	Port 2	No Link P...	100 Mbps(A)	Full(A)	Cut-through(A)	Enabled	Disabled	none
3	Port 3	No Link P...	100 Mbps(A)	Full(A)	Cut-through(A)	Enabled	Disabled	none
4	Port 4	No Link P...	100 Mbps(A)	Full(A)	Cut-through(A)	Enabled	Disabled	none
5	Port 5	No Link P...	100 Mbps(A)	Full(A)	Cut-through(A)	Enabled	Disabled	none
6	Port 6	No Link P...	100 Mbps(A)	Full(A)	Cut-through(A)	Enabled	Disabled	none
7	Port 7	No Link P...	100 Mbps(A)	Full(A)	Cut-through(A)	Enabled	Disabled	none
8	Port 8	No Link P...	100 Mbps(A)	Full(A)	Cut-through(A)	Enabled	Disabled	none
9	Port 9	No Link P...	100 Mbps(A)	Full(A)	Cut-through(A)	Enabled	Disabled	none
10	Port 10	No Link P...	100 Mbps(A)	Full(A)	Cut-through(A)	Enabled	Disabled	none
11	Port 11	No Link P...	100 Mbps(A)	Full(A)	Cut-through(A)	Enabled	Disabled	none

Figure 5.5 - Port Overview Dialog Box

2. Double-click a port to get the specific details for that port: port performance, faults, packet distribution, link aggregation and spanning tree information.

5.4.7 Stations on the Switch

Use the following procedure to view the IP addresses of the devices that have accessed management on the switch:

1. Click `Monitoring>Access Overview`.

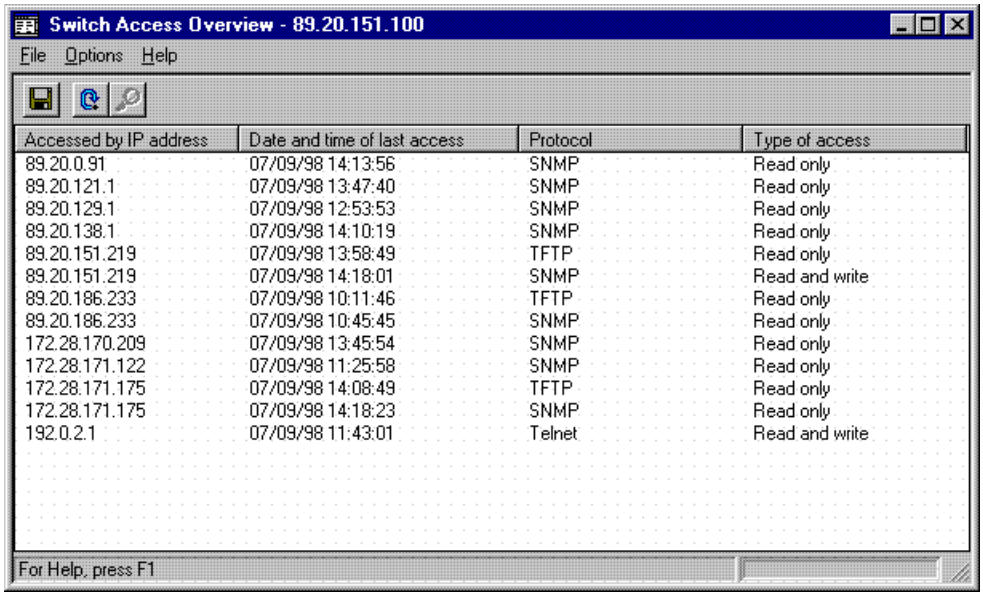


Figure 5.6 - Access Overview Dialog Box

2. To change the order of the information, click the appropriate title bar.

5.5 Monitoring Using RMON

5.5.1 Purpose

The switch contains several RMON functions. These function provide a tool for collecting information about network traffic. The following information, History, Alarm and Event Log, are switch specific. Right-click the switch to access the relevant RMON facility.

5.5.2 RMON History

Use the following procedure to monitor traffic on a subnet over a period of time:

1. Right-click a switch and select `Monitoring>RMON History`. This opens a window listing all history collections.
2. To open a graph showing the statistics, select a history and press `View`.

5.5.3 RMON Alarms

The RMON Alarm feature allows you to set your own thresholds for when the network activity requires some attention. Use the following procedure to configure RMON alarms:

1. Right-click a switch and select `Monitoring>RMON Alarms>Configure`. The `Alarm Table` window opens, which lists all alarms.
2. Click `Add` to add an alarm to the list.

   After defining the alarm, a trap is sent every time the threshold is exceeded.

5.5.4 RMON Events

The RMON Event feature allows you to set your own events, defined by type: Log, Trap or Log and Trap. Use the following procedure to configure RMON events:

1. Right-click a switch and select `Monitoring> RMON Alarms>Events`. The `Events Table` window opens, which lists all events defined.
2. Click `Add` to add an event to the list.

Events can be created automatically through alarm configurations.

5.5.5 Online Help

For more information about the use of the RMON facilities, please refer to the on-line help.

5.6 Monitoring the Stack's Performance

5.6.1 Monitoring the Health of the Stack

The Stack Health Monitor provides an overall status for the switches in the stack. To view the health of the stack, right-click the stack border and select `Stack Health Monitor`.

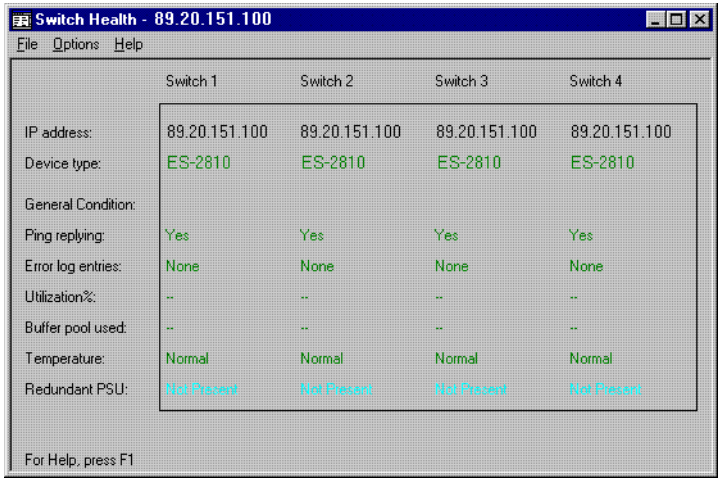


Figure 5.7 - Switch Health Dialog Box

If the condition of any of the switches changes, the changes are displayed on screen.

5.6.2 Monitoring IntraStack Activity

Use the following procedure to view the total activity of the packets between the switches in the stack, or across the Matrix Module:

1. Right-click the stack border and select `IntraStack Traffic`.

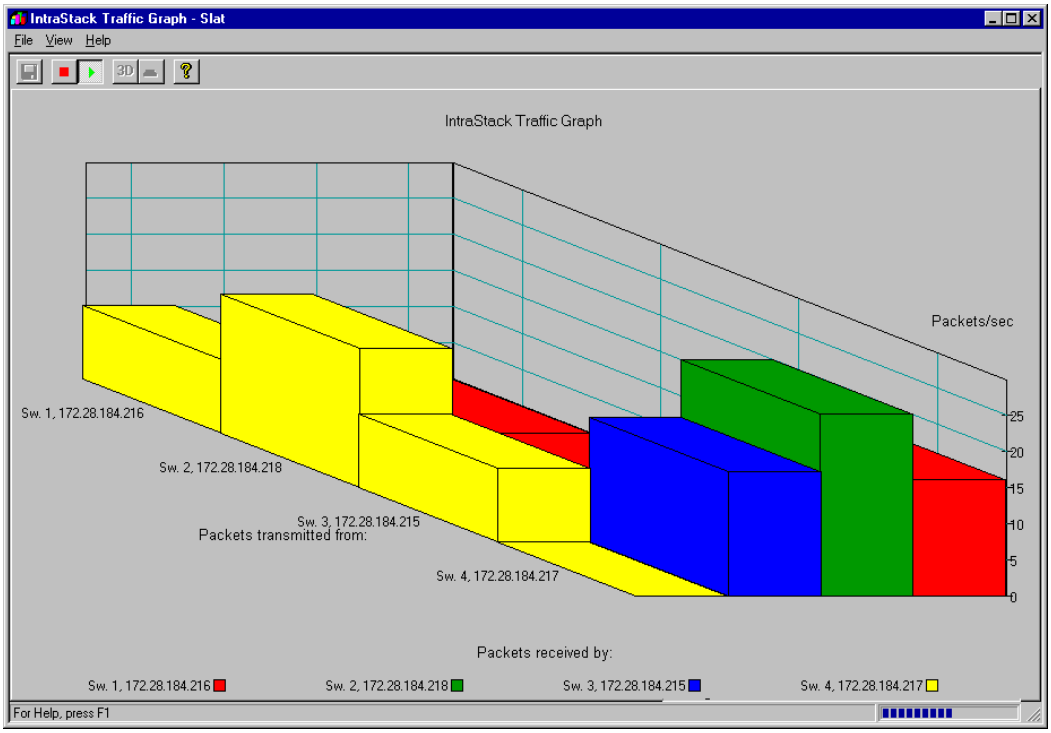


Figure 5.8 - IntraStack Traffic Graph Dialog Box

Each column represents a Matrix Module port and its activity level.

2. To see the exact value, hold the mouse pointer over a port.

5.6.3 Monitoring the Total Packet Activity per Port

Use the following procedure to view the total activity of the packets on all the ports:

1. Right-click the stack border and select `Stack Activity>Total Packets per Port`.

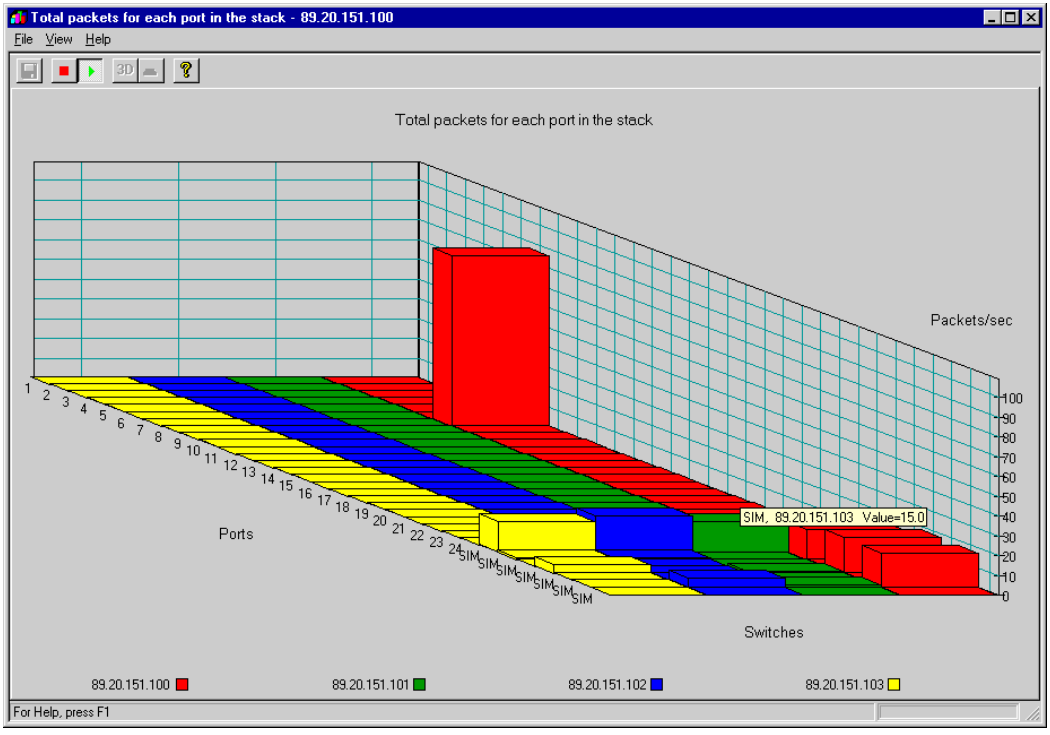


Figure 5.9 - Total Packets Graph Dialog Box

Each column represents a port and its activity level.

2. To see the exact value, hold the mouse pointer over a port.

5.6.4 Monitoring the Total Packet Activity of the Switches

Use the following procedure to view the total activity of the packets on all the switches:

1. Right-click the stack border and select `Stack Activity>Total Packets`.

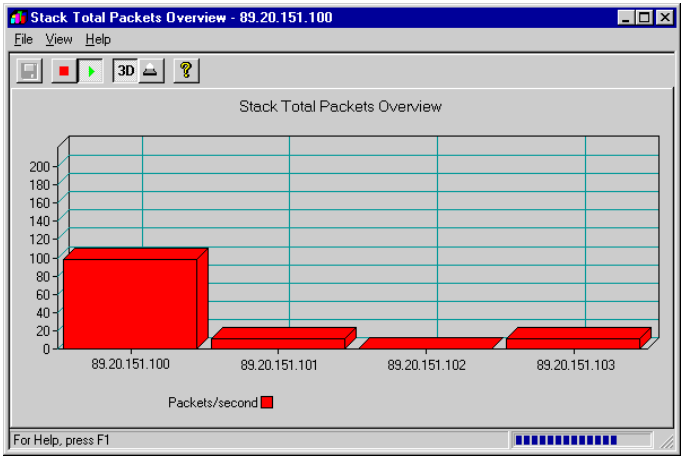


Figure 5.10 - Stack Total Packets Graph Dialog Box

   Each column represents a switch and its activity level.

2. To see the exact value, hold the mouse pointer over a switch.
3. Click `View` and change the presentation style: 3D- to 2D-Graph, with or without a peak value indicator and vertical to horizontal bars.

5.6.5 Monitoring the Total Activity of Transmitted Packets

Use the following procedure to view the total activity of the packets being transmitted on all the switches:

1. Right-click the stack border and select `Stack Activity>Tx Packets`.

   Each column represents the activity level on a switch.

2. Hold the cursor on a column to see the exact value.
3. Click `View` and change the presentation style: 3D- to 2D-Graph, with or without a peak value indicator and vertical to horizontal bars.

5.6.6 Monitoring the Total Activity of Received Packets

Use the following procedure to view the total activity of the packets being received on all the switches:

1. Right-click the stack border and select `Stack Activity>Rx Packets`.

   Each column represents the activity level on that switch.

2. Hold the cursor on a column to see the exact value.
3. Click `View` and change the presentation style: 3D- to 2D-Graph, with or without a peak value indicator and vertical to horizontal bars.

5.6.7 Monitoring the Total Number of Errors

Use the following procedure to view the total error activity of the packets on all the switches:

1. Right-click the stack border and select `Stack Activity>Errors`.

   Each column represents the activity level on that switch.

2. Hold the cursor on a column to see the exact value.
3. Click `View` and change the presentation style: 3D- to 2D-Graph, with or without a peak value indicator and vertical to horizontal bars.

5.6.8 Overview of All the Ports

Use the following procedure to view the setup configuration of all the ports in the stack:

1. Right-click the stack border and select `Port Overview`.

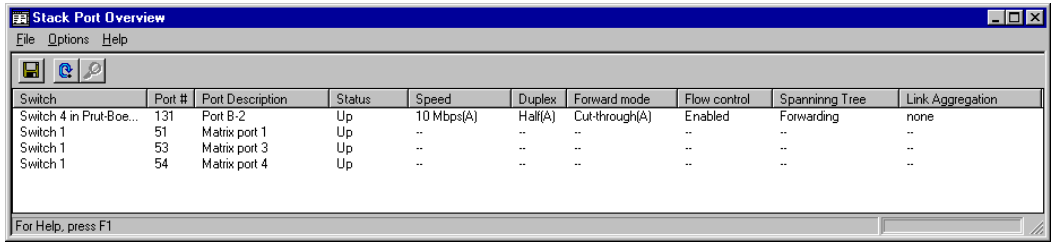


Figure 5.11 - Stack Port Overview Dialog Box

2. Double-click a port to get the specific details for that port: port performance, faults, distribution and spanning tree information.

5.6.9 Monitoring the Spanning Tree Statistics

To view the spanning tree statistics for the whole switch, right-click a specific switch and select `Spanning Tree`.

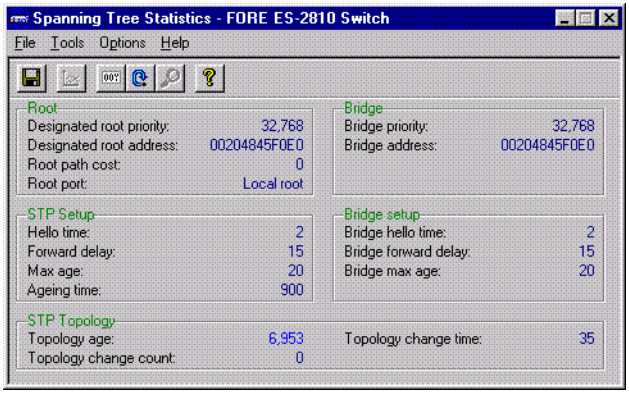


Figure 5.12 - Spanning Tree Statistics for a Whole Switch

5.6.10 Stations on the Switch

Use the following procedure to view the IP addresses of the devices on the switch:

1. Select `Monitoring>Access Overview`.

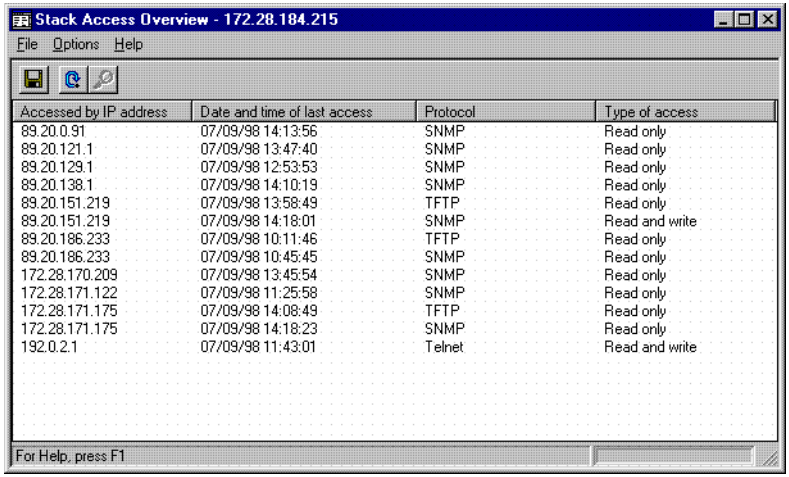


Figure 5.13 - Stack Access Overview Dialog Box

2. To change the order of the information, click the appropriate title bar.

5.7 Monitoring VLANs

5.7.1 General Information

The information provided in this section is switch specific. To get information about a switch, including switches in a stack, right-click that switch.

5.7.2 Overview of the VLANs on a Switch

Use the following procedure to view the VLANs on the switch:

1. Select `VLAN>Monitoring`.

   This shows a full list of VLANs active on the switch or in the domain (if distributed VLAN or stand-alone for a stack). To view this window from the Explorer, right-click the VLAN name and select `Monitor`.

2. Click the name of the VLAN, then click `Details` to view details of that VLAN:

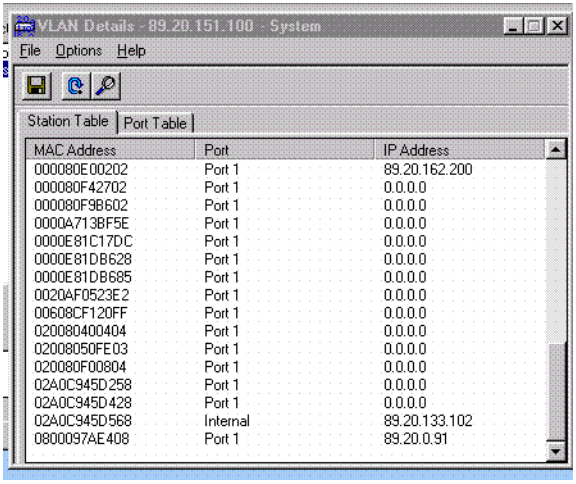


Figure 5.14 - VLAN Details Dialog Box

Click either of the tabs to view more details:

Table 5.2 - Tab Options in the VLAN Details Dialog Box

Tab Name:	Shows the VLAN's...	Double-click a row to show...
Station Table	MAC addresses, Ports and IP addresses	all VLANs in which this address is contained
Port Table	Port number and Port name	the MAC and IP address of all devices on the port in this VLAN

IP addresses will be present only if the station is learned by this switch and has sent an ARP packet.

5.7.3 Information About the Domain

Use the following procedure to view the VLAN mode and Domain name:

1. Select VLAN>Status.

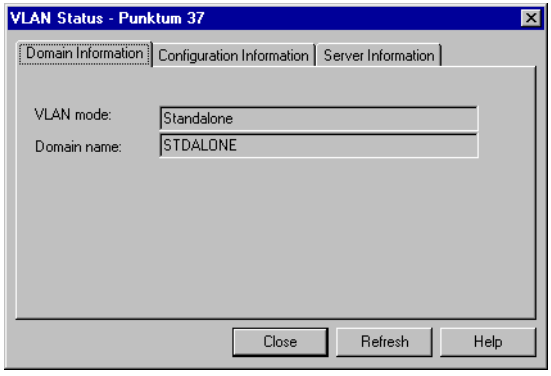


Figure 5.15 - Domain Information Tab of the VLAN Status Dialog Box

2. To change the information, see “Changing VLAN Mode” on page 4-5.

5.7.4 Information About VLAN Configuration

Use the following procedure to see if another user is configuring the VLANs, view the version number of the VLAN configuration or the time this configuration has been running:

1. Select `VLAN>Status`.
2. Click `Configuration Information`

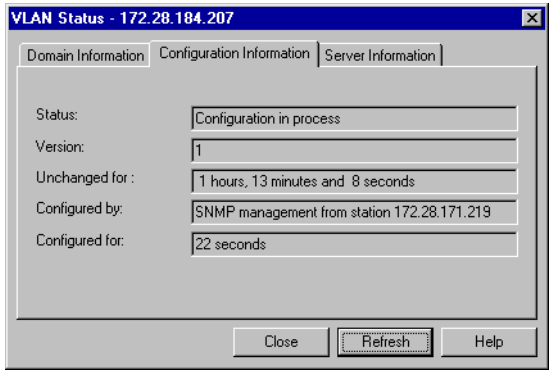


Figure 5.16 - Configuration Information Tab of the VLAN Status Dialog Box

The bottom 2 lines in this window are not displayed when the status is idle, for example nobody is editing the VLAN.

5.7.5 Information About the Server

This provides status information about the server:

NOTE

This information is only available from switches in a stack or from switches in a distributed VLAN.

1. Select VLAN>Status.
2. Click Server Information

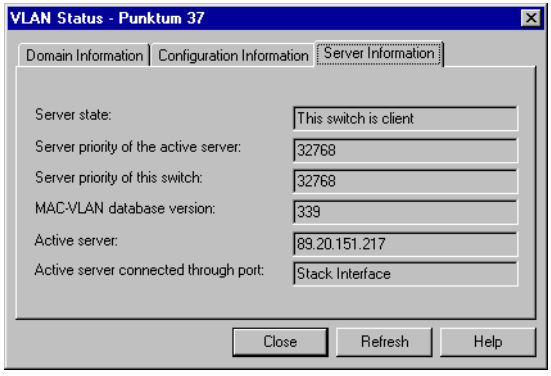


Figure 5.17 - Server Information Tab of the VLAN Status Dialog Box

5.7.6 VLAN Links to Other Switches

Use the following procedure to view the links between switches in a distributed VLAN:

This information is only available from switches in a stack or from switches in a distributed VLAN.

1. Select `VLAN>Switch VLAN Links`.

   This shows the IP address and MAC address of the other switches connected to each port in this distributed VLAN.

2. Click the appropriate title bar to change the order of the information.

5.8 Monitoring the Port's Performance

5.8.1 Using the LEDs

Using the Device View of the switch, the different colored LEDs on the ports indicate the different states of activity. Select `Help>Display Legend` for further information on LED states.

5.8.2 Monitoring the Performance of a Port

Use the following procedure to monitor the performance of a specific port:

1. Right-click the port.
2. Select `Port Details>Performance`.

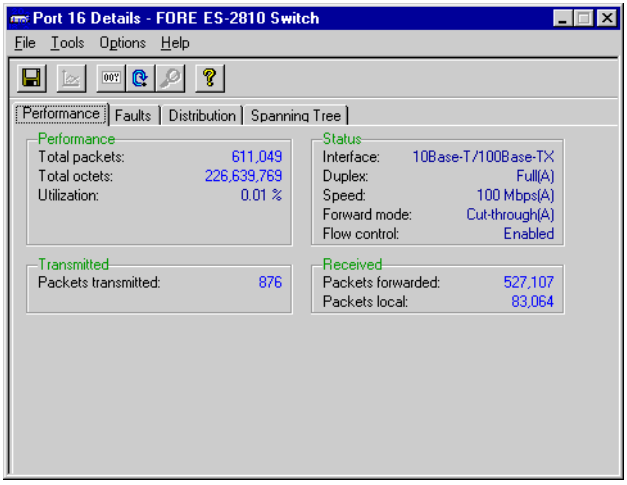


Figure 5.18 - Performance Tab of the Port Details Dialog Box

This table shows the total number of frames and bytes, utilization of the ports and the number of packets transmitted and received.

3. To change the display from numerical to graphical, click one or more of the numbers and select `Tools>Graph`.
4. Select `Options>Reset Counters` to set all these counters to zero.

5.8.3 Monitoring the Faults on a Port

Use the following procedure to monitor the faults on a specific port:

1. Right-click the port.
2. Select `Port Details>Faults`.

   This table shows the total number errors, discards and observations transmitted and received.
3. To change the display from numerical to graphical, click one or more of the numbers and select `Tools>Graph`.
4. Select `Options>Reset Counters` to set all these counters to zero.

5.8.4 Monitoring the Distribution on a Port

Use the following procedure to monitor the distribution percentages of unicast, multicast and broadcast frames on a specific port:

1. Right-click the port.
2. Select `Port Details>Distribution`.

5.8.5 Monitoring the Spanning Tree Statistics on a Port

Use the following procedure to monitor the spanning tree statistics on a specific port:

1. Right-click the port.
2. Select `Port Details>Spanning Tree`.

5.8.6 Monitoring the Received Packets on a Port

Use the following procedure to monitor the received packets on a specific port:

1. Right-click the port.
2. Select `Port Activity>RX Packets`. The Port Activity dialog box appears, as shown in Figure 5.19.

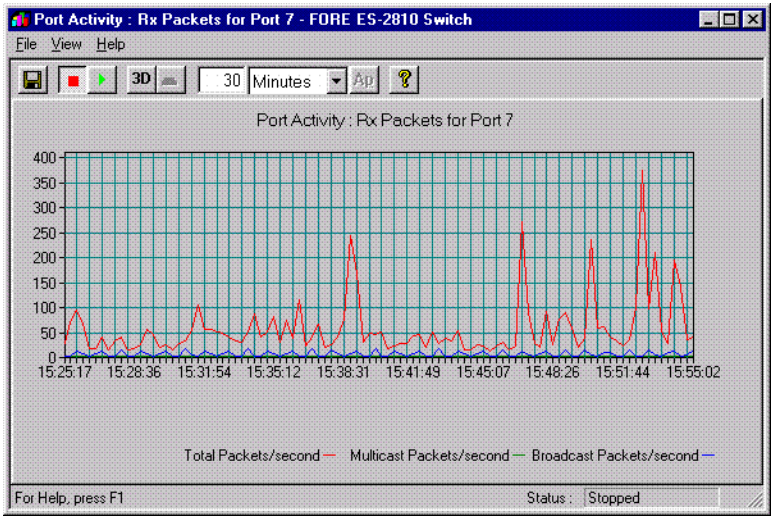


Figure 5.19 - Port Activity Graph Dialog Box

3. To change the graph, click `3D`.
4. To freeze the graph, click `View>Stop Collection`.

5.8.7 Monitoring the Packets Transmitted from a Port

Use the following procedure to monitor the transmitted packets on a specific port:

1. Right-click the port.
2. Select `Port Activity>TX Packets`.
3. To change the graph, click `3D`.
4. To freeze the graph, click `View>Stop Collection`.

5.8.8 Monitoring the VLANs on a Port

Use the following procedure to view the VLANs on the port:

1. Right-click and select `VLAN Port Monitoring`.

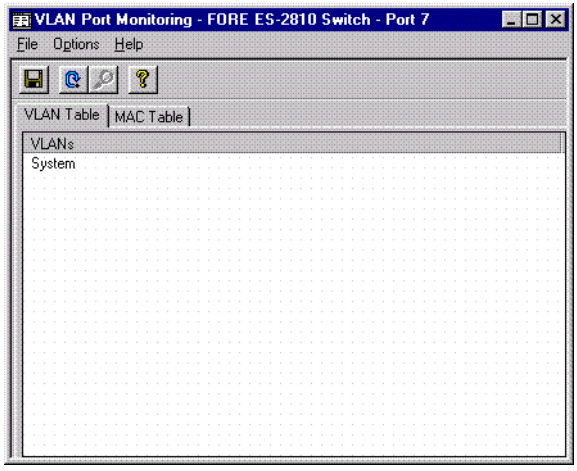


Figure 5.20 - VLAN Port Monitoring Dialog Box

2. Click either of the tabs to view details of that port, as described in Table 5.3.

Table 5.3 - Tab Options for VLAN Port Monitoring Dialog Box

Tab Name	Shows the VLAN's...	Double-click a row to show the...
VLAN Table	in which this port is contained	MAC addresses learned on this port in that specific VLAN
MAC Table	MAC addresses and IP addresses	other VLANs in which this address is contained

5.8.9 RMON Interface Statistics

Use the following procedure to access a range of subnet management statistics:

1. Right-click a port and select `RMON Statistics`.
2. This window gives more detailed information displayed as graphs.

5.9 Tools for the Switch

5.9.1 Tools Available

The switch has various tools to help with management:

Table 5.4 - Switch Management Tools

Use...	To...
Ping	Ensure a device is connected to the network.
Report Manager	Transfer files from a remote switch to your local disk or file server.
Telnet	Access the switch from any workstation on the network using Telnet.
Recovery Manager	Regain control of your switch.
DNS IP Conversion	Converts DNS names to IP addresses.

5.10 The Ping Tool

5.10.1 Pinging a Device

Use the Ping tool to ensure a device is attached to the network. If the device is on a remote network, you may need to adjust the timeout in order to receive the response.

1. Select `Tools>Ping`.

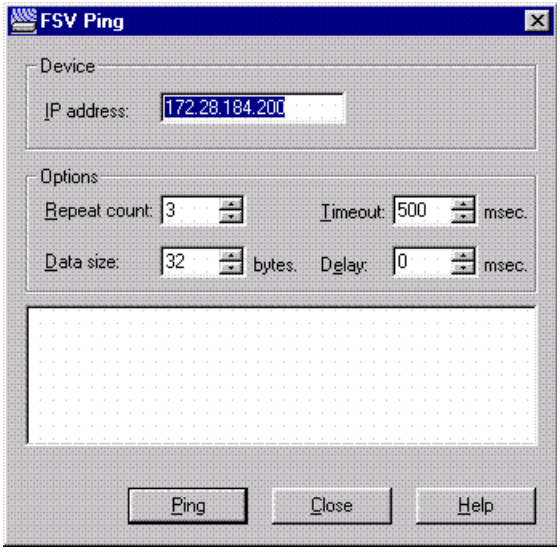


Figure 5.21 - Ping Tool Dialog Box

2. Double-click `IP Address`, and type the correct IP address for the device you want to ping.
3. Change the settings in the fields if required, and click `Ping`.

5.11 The Report Manager

5.11.1 Using the Report Manager

Use the following procedure to view a log or report:

1. Click `Tools>Report Manager`. If you are managing a stack, select the IP Address of the individual switch.

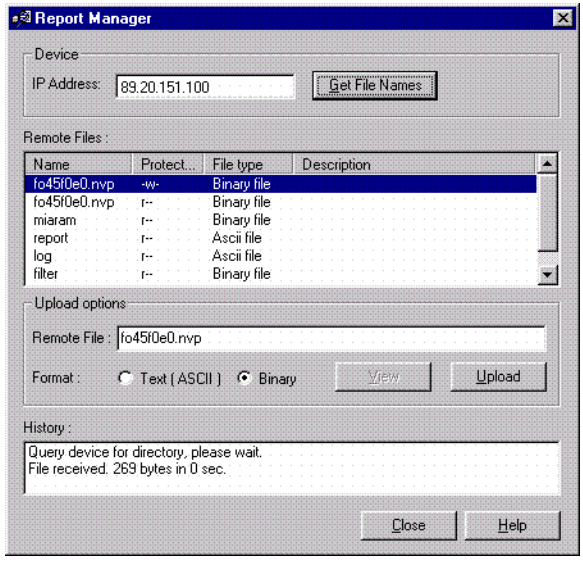


Figure 5.22 - Report Manager Dialog Box

2. Double-click `IP Address`, and type the correct IP address for the device you want to receive the directory.
3. Select a directory from the `Directory` list box, and click `View`.

5.12 The Telnet Facility

5.12.1 Purpose

The switch's Telnet facility has the following main features:

- It can be accessed from any workstation on the network using Telnet
- Access can be password protected to exclude unauthorized personnel
- Two distinct levels of management rights: administrator and user
- Log files (to pinpoint trouble sources) to provide diagnostic information for troubleshooting
- Detailed system information and operational statistics

5.12.2 What Does It Do?

This facility is divided into four parts:

- Configuration

  Allows you to change the basic configuration parameters of the switch, reset some of the configuration as well as save and load backups of the configuration.
- Monitoring shows:
  - A hardware and software overview
  - Details on messages from the system log
  - Normal traffic throughput
  - Number of errors, discards, observations and collisions for the switch
  - An overview of port-specific errors, discards, observations and collisions
  - Spanning Tree Protocol for the switch bridge and specific ports
  - MAC addresses on specific ports, and which ports have no MAC addresses
  - VLAN details

- Troubleshooting shows:
  - A diagnostics log
  - A log of errors due to software and hardware failures
  - How to overcome the limitations that exist in some management applications (RMON)
  - The option to reset all the counters being used for diagnostic purposes
  - VLAN Forced Release
- Software Update lets you:
  - Load new software to the switch
  - Reset the switch if necessary
  - Monitor the software status

5.12.3 Access to the Local Management Application

Instructions on how to access the application have been mentioned earlier:

- Access from the `CONSOLE` port

  Details are in *Quick Start*.
- Access using Telnet

  Select `Tools>Telnet`.

5.12.4 Finding the Details

After a successful login, the Telnet main menu is displayed:

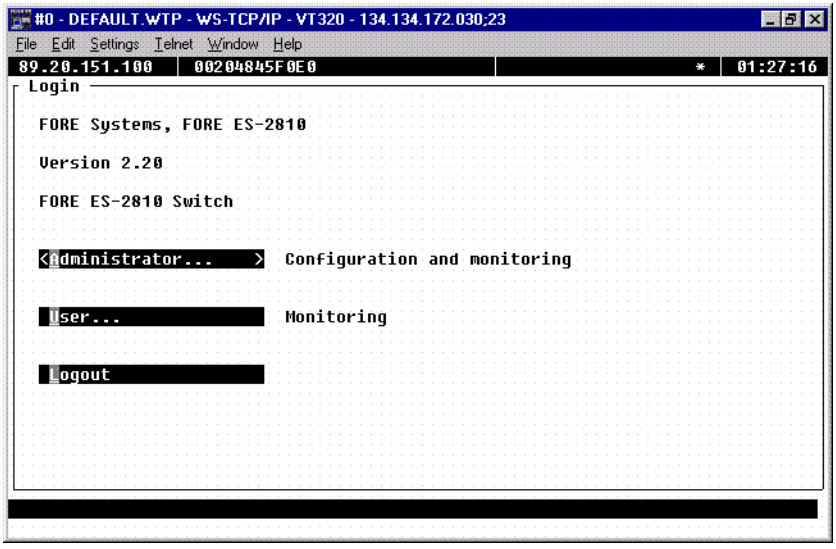


Figure 5.23 - Telnet Main Menu

5.13 The Recovery Manager

5.13.1 Purpose

Use the Recovery Manager if the software in your switch is corrupted or a software download to the switch failed, or you have moved a configured switch from another net, forgotten the switch's IP address, or simply lost control of the switch.

Figure 5.24 - Recovery Manager Dialog Box

NOTE The Recovery Mode Manager only works when the switch is set in Recovery Mode.

5.13.2 Using the Recovery Mode Manager

Use the following procedure to regain control of the switch:

1. Locate the Reset button on the front of the switch. Use a pointed object, for example a paper clip, press and hold (approximately 40 seconds) the Reset button until the Status LED blinks green slowly.
2. In FORE Stack View, select `Tools>Recovery Manager`.
3. Follow the instructions in the wizard to regain control.

5.14 DNS IP Conversion Tool

5.14.1 Using the DNS IP Tool

DNS names are resolved by a DNS server or a Hosts file. The station running FORE Stack View must be configured to use the DNS server when a Hosts file is not used. To convert DNS names to IP addresses:

1. Type in the DNS name.
2. Click `Convert.`
3. The IP address is displayed.
4. Click `Close.`

5.15 Tools for the Stack

5.15.1 Tools Available for a Stack

When managing a stack, the following tools are available:

- Stack Synchronization Manager
- Switch Position Organizer
- Color Code Matrix Ports

5.15.2 Stack Synchronization Manager

5.15.2.1 Purpose

Before switches connected together via a Matrix Module can be managed as a stack, their configurations must be synchronized. This manager checks that all the configurations are compatible. The configurations for all the switches are then synchronized from a specified switch.

5.15.2.2 Using the Synchronization Manager

Use the following procedure to start the Synchronization Manager:

1. Select `Tools>Stack Synchronization Manager`.
2. Follow the checks made and then click `Switch Selection` and select the IP address for the switch with the configuration that is to be copied to the other switches.

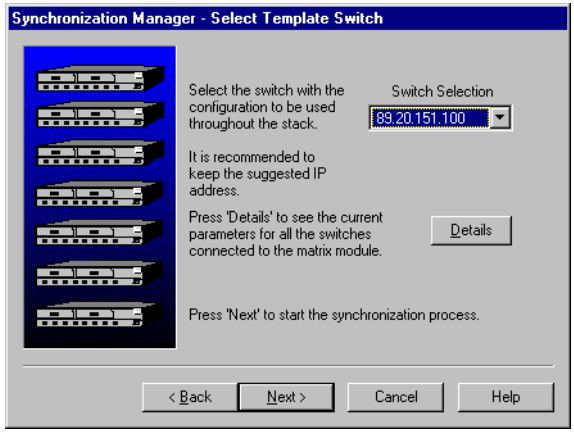


Figure 5.25 - Synchronization Manager Dialog Box

3. Click `Next>` to complete the synchronization of the switches.

5.15.3 Switch Position Organizer

5.15.3.1 Using the Switch Position Organizer

This tool enables you to reposition the switches displayed on screen, so they have the same relative position to each other as the physical switches in the stack. Use the following procedure to reposition a switch:

1. Select `Tools>Switch Position Organizer`.

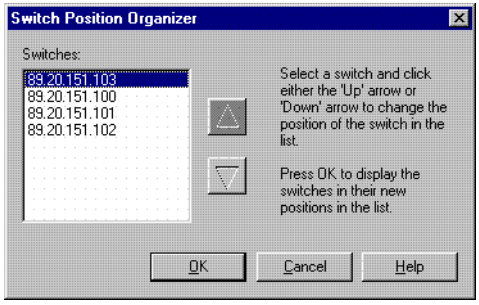


Figure 5.26 - Switch Position Organizer Dialog Box

2. Click the switch's IP address.
3. Use the arrows to change the position of the IP address in the list.
4. To update the names of the individual switches to match the physical position view, check the `Update individual switch names too`.
5. Click `OK`. The switches in Device View now change position. The new order is stored in the switch, so the order is maintained regardless of where you manage them.

5.15.4 Color Code Matrix Ports

5.15.4.1 Purpose

Enabling this tool colors the individual ports on the Matrix Module. This simplifies the task of tracing cables, as the ports on the Stack Interface Modules become the same color as the port they are connected to on the Matrix Module.

5.15.4.2 Color Coding

Each Matrix port has a unique color:

- Port 1 – brown
- Port 2 – yellow
- Port 3 – dark yellow
- Port 4 – dark cyan
- Port 5 – purple
- Port 6 – cyan
- No connection – dark gray

CHAPTER 6 Technical Specifications

6.1 In This Chapter

This chapter covers the topics described in Table 6.1.

Table 6.1 - Topics Discussed in this Chapter

Topic	See Page
Physical Specifications	page 6-2
Power Specifications	page 6-5
Performance Specifications	page 6-6

6.2 Physical Specifications

6.2.1 Approvals

Table 6.2 lists the approvals for the ES-2810.

Table 6.2 - Approvals for the ES-2810

Approval for	Standard
Safety	UL 1950 CSA-C22.2 No. 950 IEC 950 EN 60950
Emission	FCC 47 CFR part 15 Class A EN 55022 Class A CISPR 22 Class A VCCI Class 1 ITE “C-Tick” Mark CNS 13438 Class A
Susceptibility	EN 50082-1 IEC 1000-4-2 IEC 1000-4-3 IEC 1000-4-4 IEC 1000-4-5
CE Mark	Yes

6.2.2 Physical

Table 6.3 lists the physical specifications for the ES-2810.

Table 6.3 - Physical Specifications for the ES-2810

Specification	Measurement
Dimensions	Width: 17.35in. (441mm) Height: 3.26in. (83mm) Depth: 12.95in. (329mm)
Weight (approximate)	19lb. (8.6kg)
Recommended clearance	Sides: 4.0in. (100mm) Rear: 7.7in. (190mm)

6.2.3 Environmental

Table 6.4 lists the environmental specifications for the ES-2810.

Table 6.4 - Environmental Specifications for the ES-2810

Operating temperature	+41°F to +104°F (+5°C to +40°C)
Storage temperature	–13°F to +158°F (–25°C to +70°C)
Humidity	Less than 85% non-condensing
Altitude	10000 feet (3048 meters)

6.2.4 LEDs

Table 6.5 lists the number of LEDs on the ES-2810.

Table 6.5 - LEDs for the ES-2810

Status of	Number of LEDs
Port	48
Power	1
Status	1
Temperature	1
RPS	1

6.2.5 Connections

Table 6.6 list the number of connections available on the ES-2810.

Table 6.6 - Available Connections for the ES-2810

Connections	Number
10/100Mbps 10/100BaseTX (RJ-45)	24
CONSOLE port (DB-9 male)	1

6.3 Power Specifications

6.3.1 Consumption

Power consumption: 100 W maximum

6.3.2 Power Supply

Table 6.7 lists the power supply specifications for the ES-2810.

Table 6.7 - Power Supply Specifications

Nominal power supply voltages	100 to 120 V AC, 2.5 A 200 to 240 V AC, 1.5 A Class 1 protective ground
Voltage range	90 to 135 V 180 to 265 V
Frequency	47 to 63 Hz
Main power connection	Detachable power cable
Input protection	Non-replaceable, internal fuse

6.4 Performance Specifications

6.4.1 MAC Addresses

Table 6.8 lists the number of MAC addresses available on the ES-2810.

Table 6.8 - MAC Addresses Per Port

MAC addresses per port	Number of ports available for multiple addresses
Max 8000	All

6.4.2 Throughput

Internal backplane bandwidth: 2.1Gbps

6.4.3 CPU

IDT 79R3041 (16 MHz)

6.4.4 Memory Sizes

Table 6.9 lists the memory sizes for the ES-2810.

Table 6.9 - Memory Size on the ES-2810

Memory	Switch
Flash Memory (MB)	2
CPU RAM (MB)	1
Buffer RAM (MB)	4

6.4.5 Supported Protocols

Table 6.10 lists the supported protocols on the ES-2810.

Table 6.10 - Supported Protocols

Subject	Document Reference
Bridge / Spanning Tree	IEEE 802.1d
Ethernet	IEEE 802.3
Fast Ethernet	IEEE 802.3u
Full duplex flow control	IEEE 802.3x
Gigabit Ethernet	IEEE 802.3z
UDP	RFCs 768, 950 and 1071
TFTP	RFC 783
IP	RFC 791
ICMP	RFC 792
TCP	RFC 793
ARP	RFC 826
Telnet	RFC 854 to 859
BOOTP	RFCs 906, 951 and 1350
SMI	RFC 1155
SNMP	RFC 1157
MIB II	RFC 1213
Ethernet-like MIB	RFC 1398
Bridge MIB	RFC 1493
Ether-like MIB	RFC 1643
RMON	RFC 1757
IGMP version 2	RFC 1112
RSVP version 1	RFC 2205

CHAPTER 7 Console Port Use and Troubleshooting

7.1 In This Chapter

Table 7.1 lists the topics covered in this chapter.

Table 7.1 - Topics Discussed in this Chapter

7.2 Use of the Console Port

7.2.1 Purpose of Console Port

If you lose contact with the switch and the Recovery Manager in FORE Stack View or Local Management over the LAN cannot contact it, then local management and maintenance is possible via the Console port on the front of the switch.

7.2.2 Local Management

During normal operation (the switch is running and the Status LED is green) the Console port will give access to a menu, identical to the one accessible via a telnet connection to the switch. The menu allows configuration of basic parameters, extensive monitoring, flash operations, reset of the switch etc.

7.2.3 Maintenance Mode

If the switch is failing for some reason (System LED goes red), and cannot start correctly after a reset, this could be caused by either hardware failure, corruption of the software, or corruption of the switch configuration. The maintenance mode is provided to allow recovery from a situation when the Recovery Manager of FORE Stack View cannot be applied. In the following sections, various problems are described as well as solutions using maintenance mode. “Using Maintenance Mode” on page 7-6 describes how to start and use the maintenance mode.

Loading software to the switch in Maintenance Mode should only be done as a last resort, the reason being that the software and configuration are already resident in the flash memory is overwritten and lost.

7.2.4 Switch Software

The software for the switch (including a default configuration) resides in the switch’s flash memory. A backup of the software is provided on the CD delivered with the switch, and the newest software versions may be downloaded via the Internet. The software files may be used for restoring or upgrading the switch software.

7.2.5 Restoring Software

The switch software may be restored / downloaded from a TFTP server, if the current software in flash memory has been corrupted. The TFTP and BOOTP commands may both be used to accomplish this. For the TFTP command an external TFTP server with the software must be present on the network. For the BOOTP command a BOOTP / TFTP server (often referred to as a boot server) must be present.

7.2.6 Upgrading Software

If working switch software needs to be upgraded, FORE recommends using the Software Upgrade Wizard in FORE Stack View rather than the maintenance mode commands. This is easier and the existing configuration is retained.

7.2.7 Switch Configuration

The configuration information for the switch is stored in two files residing in flash memory. The two files are named after the MAC address of the switch:

- `ixxxxxxx.p` contains all the basic configuration parameters
- `dxxxxxxx.nvp` contains the VLAN policy database.

7.2.8 Backing up the Configuration

The two configuration files may be backed up using a TFTP client on an external machine (e.g. MS Windows*, Unix* or other). Please follow the documentation for the TFTP client application for further instructions. However, it is recommended that you use FORE Stack View for doing backup of the configurations.

7.2.9 Restoring the Configuration

The two configuration files may be restored using a TFTP client on an external machine (e.g. MS Windows*, Unix* or other), if the switch configuration has been lost or corrupted. It is recommended that you use FORE Stack View for restoring the configurations rather than manual TFTP.

7.2.10 Reset to Factory Defaults

If the configuration in the switch has been corrupted in such a way that the switch is not able to start properly after reset (System LED goes red), it may be necessary to reset the switch configuration to factory defaults. The **`RUN Defparm`** command can be used to do this. Note that this will discard the existing configuration in the switch. This method can also be used if the configuration by mistake has made it impossible to contact the switch by other means. It is also the only way to regain access to the switch if the administrator password has been lost.

7.3 Recovering from Start-up Failure

7.3.1 Network Boot Process

The network boot process is as follows:

1. The switch sends a BOOTP request over the network.

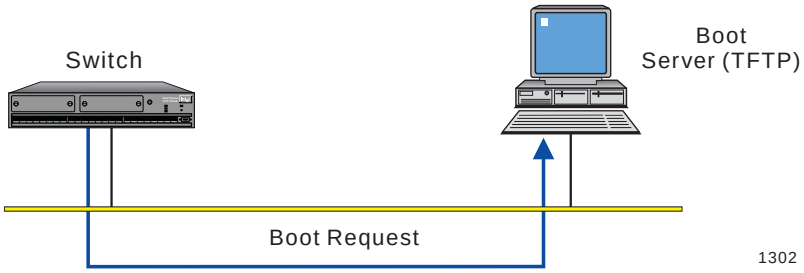


Figure 7.1 - BOOTP Request

The boot request contains the switch's MAC address. The boot server contains a bootptab file with an entry for the switch which is defined by the MAC address.

2. If a boot server which holds the software for the switch receives the boot request, it loads the boot software over the network to the destination MAC address.

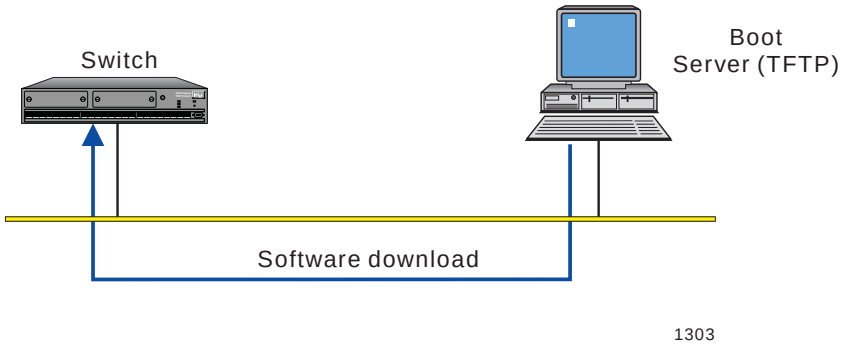


Figure 7.2 - BOOTP Process

7.4 Using Maintenance Mode

7.4.1 Purpose

Maintenance Mode offers three facilities:

- It allows you to force the switch to load a specified software file from any specified TFTP server.
- It provides an emergency facility to force boot the switch from a specified boot server if the switch cannot boot from Flash Memory. From Maintenance Mode the switch is forced to issue a BOOTP request with the name of the boot software to a specified boot server. This is useful if the boot server being used does not support the use of a bootptab file.
- It runs tests on hardware and provides diagnostic information.

Loading software to the switch in Maintenance Mode should only be done as a last resort. This is because the software and configuration already resident in the flash memory is overwritten and lost.

7.4.2 Important Considerations

Consider these points when using Maintenance Mode:

- The switch is not operational and the expansion board ports cannot be used.
- Only simple command-line access is possible via the `Console` port.
- There is a delay before you see the command prompt; this is due to a hardware test routine being completed.

7.4.3 To Enter Maintenance Mode

To enter Maintenance Mode:

1. Using a pointed tool — such as a bent paper clip — press the **Reset** button on the front of the switch and hold it until the SYSTEM LED flashes green quickly (five times per second).
2. Release the **Reset** button.
3. Attach a VT100-compatible terminal to the serial port on the front panel using the cable supplied.
4. To display the command prompt on screen, press the **<Enter>** key a couple of times.

7.4.4 Commands Allowed in Maintenance Mode

The following command is available for the switch in Maintenance Mode:

Table 7.2 - Commands Available in Maintenance Mode

Command	Use
TFTP <filename> ownIP tftpIP [gwIP]	
	Loads software using the TFTP protocol
	<filename>: the name of the file containing the software
	ownIP: your own IP address
	tftpIP: the IP address of the TFTP host
	[gwIP: the IP address of the primary router (intermediate gateway)— required if the TFTP server is located on a remote part of the network
BOOTP <filename>	
	Loads software using the BOOTP or TFTP protocol
	<filename>: the name of the file containing the software
DUMP addr	Dumps memory contents
INFO	Shows hardware information
RESET	Resets the switch
RUN defparm	Starts the software in its default factory settings

7.4.5 Bootptab File Entry

The entry for the switch in the `bootptab` should contain a line similar to:

```
:bf=/FORE/switch/es2810_x.xx:
```

This instructs the switch to load the switch software from the bootp / tftp server. Use the FORE Stack View application to configure the switch manually, or transfer the `ixxxxxxx.p` file containing the configuration from a TFTP server to the switch.

7.5 Troubleshooting Tools

7.5.1 Troubleshooting Tools Available

The tools available for troubleshooting on the switch are:

7.5.1.1 The LED Indicators

These are located on the front panel of the switch. The LEDs indicate the overall switch status, and the status of each of the switch's ports and backplane segments (where applicable). See earlier in this manual for a full description of the LEDs and their use.

7.5.1.2 SNMP

SNMP management in the switch is based on standard Management Information Base (MIB) II and Private Enterprise MIB extensions.

You can configure the switch to send SNMP Traps to defined locations, thus allowing the possibility of performing limited troubleshooting from an SNMP Management Center.

7.5.1.3 FORE Stack View

FORE Stack View offers several features that can help your troubleshooting. These include:

- Diagnostic messages
- A log of system events
- A log of errors
- A list of SNMP traps.

7.6 Troubleshooting Procedure

7.6.1 Isolating the Problem

7.6.1.1 To Isolate the Problem

If the switch has a problem, use the following procedure to isolate the problem:

1. Check the LEDs.

   The LEDs provide instant visual indication of the status of the switch and the status of each ports.

2. Check the `Diagnostics` window.

   The diagnostics tool automatically detects possible problems and indicates possible causes and solutions. Use of this tool is described in "Diagnostics Window" on page 2-28.

3. Check for any relevant messages in the `Trap` window.

   Use of this tool is described in "Diagnostic Details Dialog BoxTrap Window" on page 2-30.

4. Check for any relevant messages in the `System` window.

   The System Log gives details about system events that occur during start-up and operation and also the general state of the switch. Typical information recorded in the System Log includes all major events during start-up, system changes, unexpected events and configuration errors. The System Log reports such things as software successfully located and loaded, ports enabled or disabled, and if any SNMP traps have been sent. Use of this tool is described in "System Window" on page 2-31.

5. Check for any relevant messages in the `Errors` window.

   Use of this tool is described in "Errors Window" on page 2-32.

6. Check the fault counters on the switch ports and watch for any significant error counters.

7.6.2 Further Evaluation of the Problem

If you still cannot resolve the problem after following the procedures above, access the Monitoring menu within Local Management. Monitoring is a valuable tool for the troubleshooting process and offers extensive information on the performance and the status of the switch hardware and software, the switch ports and the traffic patterns on each port.

The general facilities available within the Monitoring menu are described in the following subsections. The use of these facilities depends on the problem and on any relevant information collected in the previous procedure.

7.7 Typical Problems and Causes

This section gives some examples of typical problems that could be encountered during the installation and configuration of the switch, and their possible cause. Configuration problems, defective cables and problems with communication among devices are the most common switch malfunctions.

7.7.1 Start-up Problems

I've forgotten my password

- ***Explanation:*** You are prompted for a password on the `Login` screen.
- ***Action:*** Enter Maintenance Mode, and type: `run defparm`.

  This resets the configuration to the default values so you can assign a new password.

When I make changes to the switch's configuration, they take effect but as soon as the switch is powered off and on again the changes are lost

- ***Explanation:*** When you change the switch's configuration, you are changing the current active configuration that is running in RAM. However, every time the switch starts up it loads the configuration that is stored in its flash memory. Therefore, if you make a change to the configuration and want to keep it, you need to save the new configuration to the switch's flash memory.
- ***Action:*** Save the configuration changes to flash memory.

  To check the status of the configuration, select `Configuration>Software`.

7.7.2 Performance Problems

One or more workstations cannot communicate with a server or other device through the switch

- ***Explanation:*** This symptom might be noticed on one or more segments connected to the switch, and could be caused by cable faults, inappropriate configuration or faulty installation.
- ***Action:*** Check all connections and verify your configuration. Check any error counters for the ports.

The 100Mbps ports are not working, or work very poorly

- ***Explanation:*** This is probably due to incorrect configuration of the auto-negotiation duplex settings and link speeds.
- ***Action:*** Check the negotiated settings in the switch and compare them to the expected values.

I have poor performance and high numbers of second port drops

- ***Explanation:*** There may be a loop in the network and Spanning Tree is not enabled.
- ***Action:*** Avoid loops, or alternatively, either enable STP on all the ports (using `Device Setup`) or specific ports (using `Port Setup`).

7.7.3 Communication Problems

7.7.3.1 The Most Common Problems are Cable Problems

A high percentage of faults are caused by cable faults such as loose connections or inappropriately wired cables.

7.7.3.2 Spanning Tree Topology Changes

When a change is detected in the Spanning Tree network, the devices forming the Spanning Tree go into a learning state to determine the optimal routes between network segments. During this learning state, the switch will not forward data traffic.

This is a normal occurrence for Spanning tree devices and no remedial action is required. However, if the switch goes into the learning state too frequently, the Spanning Tree may be unstable and should be examined and possibly reconfigured.

7.7.3.3 To Troubleshoot Communications Problems

If the POWER LED and the STATUS LED are both on, but one or more of the port STATUS LEDs are off, then:

1. Reset the switch using the Reset button.
2. Check the STATUS LED for each switch port to which a cable is attached.

7.7.3.4 VLANs

The use of VLAN policies can lead to unexpected communication problems. If the policies are not designed with care, ports are not able to reach network services. Check your VLAN policies and use the VLAN monitoring to review the VLAN membership for that port or address.

7.8 Contacting the Technical Assistance Center (TAC)

7.8.1 Introduction

If you are unable to solve the problem and want to report the problem to FORE's Technical Assistance Center (TAC), there are certain things that you can do, to enable us to begin solving your problem quickly. FORE Stack View makes the gathering of such information easy, and presents it in an easy-to-interpret format.

7.8.2 Things to do Prior to Contacting TAC

To ensure that your problem gets treated as efficiently as possible. TFTP a report and parameter block from the switch. If it is not possible to TFTP from the switch, try to obtain the product number and the software ID and version number, any error messages in the Error and System Logs, and a copy of the switch's configuration.

Always supply the following information when contacting TAC for help:

- The scope and characteristics of the problem. How severe is the problem? Is the switch dead? Are any of the ports malfunctioning? If so, which ports? Is the whole network down?
- A quick sketch of your configuration.
- Is the problem reproducible? If yes, how?
- Is it a new installation, or has it been running for a while?
- When was the last time it was working correctly? What has happened since then that might have affected the switch?

The information in this report will help us to find a solution to the problem as quickly as possible.

7.8.3 Further Information on TAC

For information about FORE's support service, refer to "Technical Service".

7.9 Retrieving Information for the TAC

7.9.1 Two Methods Available

If FORE Stack View is still functioning, this information can be obtained using the Report Manager. If the Report Manager is not accessible, use TFTP procedures.

7.9.2 Files Suitable for TFTP Transfer

You can retrieve log files for analysis using TFTP. Here are two of the various files suitable for TFTP transfer:

Table 7.3 - Log Files Suitable for TFTP Transfer

Type	Name	Contains
ASCII	`report`	Information for the Technical Assistance Center (TAC)
	`log`	List of errors
Binary	`miaram`	Information for the Technical Assistance Center (TAC)
	`filter`	
	`i`*`xxxxxx`*`.p`	For example `in9eb003.p` A read/write parameter file which contains the information for configuring a switch somewhere else on the network.
	`i`*`xxxxxx`*`.nvp`	VLAN database

7.9.3 Transferring Files to and From the Switch using TFTP

To transfer files using TFTP:

1. At the command prompt, start a TFTP session with the switch.
2. To obtain a directory listing of all the files on the switch, type: **`get dir`**.
3. Examine the directory listing to confirm the names of the files present in the switch.

   Report, log and filter files and a parameter file with a `.p` or `.nvp` extension appear in the directory listing.
4. To retrieve the file that you want, type: **`get <`***`filename`***`>`**.

If you "get" a report, then the report file is generated on-the-fly and transferred.

5. If the TFTP access is password protected, type:

   `get<`*`password`***`>/<`***`filename`***`>`**

   For example, **`get edinburgh/report`**.

APPENDIX A Concepts in Switching

This appendix gives a introduction to the concepts behind the features in the switch:

- Forwarding Mode

  Each port can operate in adaptive, cut-through, fragment-free or store-and-forward forwarding mode. A description of each of the forwarding modes and when to configure them is given in “Forwarding Modes” on page A-2.
- Flow Control
- You can select half- or full-duplex for each port. This is described in “Half- and Full-duplex” on page A-8.
- Auto-negotiation
- Port Filters
- Internet Protocol
- Give the switch an IP address for use in SNMP and TFTP. For details see “IP Addresses” on page A-16.
- Spanning Tree
- Configure the Spanning Tree priorities and costs associated with use of the switch and ports. For details see “Spanning Tree” on page A-20.
- Permanent MAC addresses
- Virtual LANs (VLANs)

A.1 Forwarding Modes

A.1.1 Forwarding Mode Affect on Latency

Latency is the delay measured from the time the packet first enters a network device until it leaves it. The closer a device is to zero latency, the better.

The type of network can affect latency. Over wide area networks, latency is negligible in comparison to the time it takes the signals to travel over long distance lines. On local area networks, reducing latency normally increases performance.

Unfortunately, reducing the latency can often lead to an increase in errors on the network. The ideal situation is

Change the forwarding modes to provide added reliability and flexibility. For example, if you are concerned about the generation of errors on a network, you can configure the ports to store-and-forward mode to ensure safe transfer of data.

A.1.2 Possible Forwarding Modes

You can specify one of four possible forwarding modes you can specify for each port:

- Cut-through
- Fragment-free
- Store-and-forward
- Adaptive

A.1.3 Forwarding Policy

If two communicating ports (receive port and transmit port) have different forwarding modes, then they use the “safest” mode. For example, if one port is configured for fragment-free and the other port is configured for store-and-forward, then traffic between the two ports in either direction is always switched using store-and-forward.

A.1.4 CRC Errors

Cyclic Redundancy Check (CRC) errors are the sum of Frame Check Sequences, longs, very longs, alignment errors and jabbers.

A.1.5 Fragment

A fragment is a frame consisting of only part of a packet; these can be caused by collisions on the network and are normal occurrences.

A.1.6 Cut-through Forwarding

Cut-through forwarding sends the packet to the destination as soon as the first 14 bytes of the packet are read—an approximate latency of 30 microseconds for 10Mbps devices and 11 microseconds for 100Mbps devices. The delay is minimal and the packets reach their destination in the shortest possible time.

The packets are sent through the switch as a continuous flow of data—the transmit and receive rates are always the same. Because of this, cut-through forwarding cannot pass packets to higher speed networks, for example, to forward packets from a 10Mbps to a 100Mbps Ethernet network.

Since the switch has forwarded most of the packet when the CRC is read, the switch cannot discard packets with CRC errors. However, the CRC check is still made and, if errors are found, the error count is updated.

Cut-through forwarding is recommended for networks intended to provide one switch port per user, or for lightly loaded networks. It is essential for multimedia applications and ideal for workgroup environments where minimum delays are required.

A.1.7 Fragment-free Forwarding

Fragment-free forwarding is suitable for backbone applications in a congested network, or when connections are allocated to a number of users.

Fragment-free forwarding checks that there are no collisions within the first 64 bytes of the packet—the minimum valid message size required by the IEEE 802.3 specification. This guarantees that message fragments less than 64 bytes (runts) are not forwarded to other network segments. Runts are typically the result of collision fragments.

The packets are sent through the switch as a continuous flow of data—the transmit and receive rates are always the same. Because of this, fragment-free forwarding cannot pass packets to higher speed networks, for example, to forward packets from a 10Mbps to a 100Mbps Ethernet network. Therefore, if you opt for fragment-free forwarding, you cannot make direct connections to higher speed networks (like FDDI) from that port.

Fragment-free forwarding offers a compromise between cut-through (which offers the fastest possible forwarding at the expense of error checking) and store-and-forward (which offers maximum error checking at the expense of forwarding speed), to provide a latency of approximately 60 microseconds and sufficient error checking to eliminate the most common errors.

A.1.8 Store-and-forward Forwarding

Store-and-forward forwarding temporarily stores a packet and checks it against the CRC field. If the packet is error free, it is forwarded; otherwise, it is discarded.

Store-and-forward forwarding is therefore the best forwarding mode to prevent errors being forwarded throughout the network. The buffering used by store-and-forward also allows the switch to dispatch packets at a different rate than it receives them—for example, to forward packets from a 10Mbps network to higher speed networks such as a 100Mbps Ethernet.

A.1.9 Adaptive Forwarding

Adaptive forwarding mode is a user-defined facility to maximize the efficiency of the switch. Adaptive forwarding starts in the default switch forwarding mode you have selected in the `Switch & Port` window (cut-through if you selected adaptive mode as the default forwarding mode). Depending on the number of runts and CRC errors at that port, the mode changes to the "best" of the other two forwarding modes. As the numbers of runts and CRC errors change, so does the forwarding mode. This is best illustrated by:

Table A.1 - Adaptive Forwarding Modes

Forwarding mode:	Detects:	Then, adaptive mode changes the forwarding mode to:
Cut-through	High numbers of CRC errors	Store-and-forward
	High numbers of runts	Fragment-free
Fragment-free	High numbers of CRC errors	Store-and-forward
	Low numbers of runts	Cut-through
Store-and-forward	Low numbers of CRC errors	Fragment-free
	Low numbers of CRC errors and runts	Cut-through

While CRC errors and runts are the most likely parameters to cause the forwarding mode to change, they are not the only ones.

A.1.10 Latency

Delays depend on the forwarding mode:

Table A.2 - Latency Periods for Forwarding Modes

	Cut-through	Fragment-free	Store-and-forward
Min. Latency (in microsec.)	Low (10 Mbit is < 30 100 Mbit is < 11)	Medium (< 60)	High (Depends on packet size)
Amount of packet read	14 bytes: Destination address + Source address + Type / Length field)	64 bytes (IEEE 802.3)	All (CRC)
Error detection	None	Runts	All
Suitable for	One user per port. Light loads. Applications requiring low latency forwarding.	Many users on one connection. Congested networks.	Communication with higher-speed networks. A port with many errors.

A.2 Flow Control

A.2.1 Flow Control Concept

The switch can become overloaded if incoming frames arrive faster than the switch can process them, and this results in the frames being discarded until the overload condition passes. The flow control mechanism overcomes this problem and eliminates the risk of lost frames.

If a potential overload situation occurs, the switch simply generates a “pseudo collision” which forces all transmitting stations to immediately stop transmitting and wait a random amount of time before trying to retransmit. Followi7ng a simulated collision, any buffered frames are sent to their destination—clearing the switch’s buffers and allowing it to receive future frames.

A.2.2 When to Use Flow Control

The flow control mechanism is ideal for situations where only one station is attached to one switch port—do not use flow control on a port connected to a hub. However, consider the case where there is more than one station attached to a port as shown below:

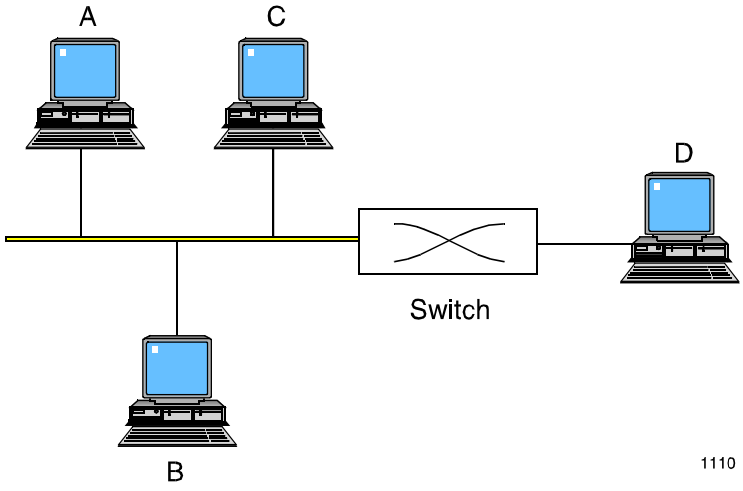


Figure A.1 - Flow Control

If station C tries to send data to station D via the overloaded switch, station C is "invited" to stop transmitting and wait a random time before trying again. Because stations A and B are on the same cable segment as station C, they also detect the collision and are therefore also prevented from sending data to each other (not just to station D), for as long as the switch is overloaded.

Flow control influences all ports that have flow control enabled—regardless of which port(s) is responsible for the overload situation.

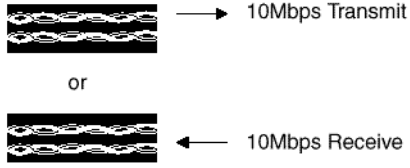
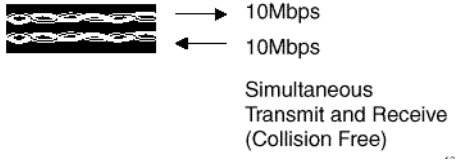
A.3 Half- and Full-duplex

A.3.1 Half-duplex and Full-duplex Concepts

Half-duplex works optimally only if one device is transmitting and all the other devices are receiving—otherwise, collisions occur. When the collisions are detected, the devices causing the collision wait for a random time before retransmitting. This means that at half duplex, Ethernet throughput is limited by the need to retransmit data when collisions occur. Half-duplex is the most common transmission method and is adequate for normal workstation and PC connections.

Full-duplex provides dual communication on a point-to-point connection and allows each device to simultaneously transmit and receive on a connection. Full-duplex mode is typically used to connect to other switches or to connect fast access devices such as workgroup servers.

Table A.3 - Half-duplex and Full-duplex

Transmission mode		Capacity
Half-duplex		Less than 10Mbps when communicating
Full-duplex		20 Mbps

NOTE

To use full-duplex communication, both ends of the connection must be configured to operate in full-duplex mode, and the connecting device must have a full-duplex adapter installed. Full-duplex operation is only possible on point-to-point Ethernet connections that use separate conductors or fibers for transmit and receive, such as 10Base-T and 100Base-FX cabling. Full-duplex operation is not possible on connections using coaxial or AUI (10Base-5) cables or with most hubs.

A.3.2 When to Use Full-duplex

Some servers perform better using full-duplex because they simultaneously handle traffic from many clients: some are transmitting data to the server, while others are receiving data from the server. Switch-to-switch connections certainly benefit from full-duplex transmission.

Individual workstations normally run applications traditionally written for half-duplex, request/response network connections, and are unlikely to benefit from being configured as full-duplex. For example, the application may request a service on a server and then wait for a reply before continuing operations. In this case, if the server connection was full-duplex, the server might respond to the request while simultaneously receiving from another station; a full-duplex connection for the workstation would typically offer no advantage.

A.3.3 Auto Duplex

Auto duplex negotiates whether the attached device is transmitting in half- or full-duplex, and then automatically changes that port to that mode.

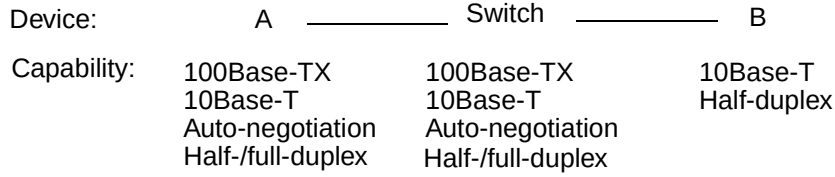
A.4 Auto-negotiation

A.4.1 Auto-negotiation Concept

Auto-negotiation follows the IEEE 802.3u 100Base-T specification to improve the effectiveness of dual speed links (such as the base ports and the 10/100TX Media Module). They have the capability to work at either of their speeds (10Mbps or 100Mbps) and either of the duplex modes (half- or full-duplex).

Normally you would need to configure the port on the switch with a specific speed or duplex mode, but that is not required with auto-negotiation — it detects the capabilities of the other devices (over a common link) and configures itself to use the same technology automatically; this gives maximum efficiency.

To illustrate how auto-negotiation works, imagine two devices connected via a switch as shown in the figure below.



Auto-negotiation allows the Switch port to select the best transmission speed and duplex mode—based on the capabilities of the device at the other end.

The link between Device A and the Switch has Auto-negotiation enabled at both ends. Since both ends support 100Mbps full-duplex mode, this mode is selected.

Device B is also connected to the Switch, but only supports 10Mbps half-duplex transmission. The Switch automatically detects this and select 10Mbps half-duplex transmission for this port.

A.4.2 Checklist for Problems

If you have problems with auto-negotiation, here are some helpful hints:

- If there is no link pulse:
  - Check the cable
  - Check auto-negotiation setup
  - A match must exist between the stations
- If the port is disabled:
  - Check that the configuration of the port is correct
  - Check that the modes you have entered match
  - For example, Speed is used during auto-negotiation

A.5 Port Filters

A.5.1 Introduction

It is possible to increase network security by using port filters. Adding a filter to a port determines where data can come from (using port numbers and MAC addresses) and go to (using port numbers and MAC addresses) on the network. This means that you can have a high level of network security.

A.5.2 Purpose

The Port / MAC Filter facility lets you:

- Specify which ports the MAC address can be learned on
- Specify which ports the MAC address can send packets to
- Specify which ports can receive Multicast packets
- Send packets from one port to other specified ports
- Change the information on an existing port or MAC address
- Delete filtering on an existing port or MAC address
- Enable or disable the filtering system
- Scan the specifications you have made to detect any trivial errors

A.5.3 Conflicts with Other Settings

When you add or make changes to Port / MAC filter settings, it is possible it may conflict with VLANs or permanent MAC address settings in other windows of the switch. To reduce the danger of altering the switch configuration by mistake, certain priorities have been made. These are listed in “Port Filter Priorities” on page A-15.

A.5.4 Add a Port Filter

A.5.4.1 Introduction

You can add up to 100 filters. When you add a filter, you choose from the ports available at that time. If more ports are added later (for example, by connecting an expansion module), you should edit your filters to include the new ports.

When you remove ports (for example, disconnecting the expansion module), those ports are removed from the filter set-up. If these ports are the only ones in the source or destination port list, the filter is deleted.

If you choose all the ports available, the screen shows `All` in the list. If you then connect an expansion module—thus adding ports that are not in that filter—the ports are listed individually.

To show that a source port is not required for the filter, "--" is used in the `Source ports` list.

A.5.4.2 Types of Port Filter Entry

There are three types of port filter entry:

- Port relation
- MAC unicast
- MAC multicast

A.5.5 MAC addresses

A.5.5.1 Entering a MAC Address

There are limited options when entering a MAC address:

Table A.4 - MAC Address Options

Enter	Possible?	Explanation
Broadcast address (FFFFFFFFFFFF)	No	This address must be available to all ports.
STP Multicast (0180C2000000)	No	This multicast is used for switch functions.
Limit flooding of Multicast addresses to certain ports	Yes	Create a filter (for the corresponding Multicast address) with destination ports specified. The multicast is only transmitted to these ports on the switch.
Multicast kept within existing VLAN	Yes	VLAN constraints.

A.5.5.2 Violation of Port/MAC Filter

If a MAC address violates the Port/MAC filter setting, an error message shows the offending MAC address and the port on which the violation occurred. An SNMP trap containing the port number is also sent on the network.

A.5.5.3 The Switch's Own MAC Address is Part of a Filter Entry

This entry is ignored by the filter and an entry in the error log indicates what happened.

A.5.6 Port Filter Priorities

A.5.6.1 Introduction

When you make changes to VLANs or permanent MAC addresses in other windows of the switch, it is possible you may have conflict between the Port / MAC filter settings and other settings. To reduce the danger of altering the switch configuration by mistake, certain priorities have been made.

A.5.6.2 VLANs

A port VLAN always has priority over a Port / MAC filter setup. When you add or change a filter setup, you can only specify ports that belong to the same VLAN; this ensures the packets never go beyond the limits of that VLAN.

A.5.6.3 Permanent Port Entries

A permanent MAC address on a port always has priority over a Port / MAC filter setup. When you add or change a filter setup, you can only specify the port that is the permanent MAC address.

A.5.6.4 To Remove Conflicting Setups

When you change to a VLAN or permanent MAC address entry, the switch automatically checks for configuration conflicts with the Port / MAC filters. If a conflict exists, you have two options:

- Change the VLAN or permanent MAC address setup:

  This removes the conflict between the setups
- Keep the VLAN or permanent MAC address setup:
- This automatically disables the Port / MAC filtering

If the Port / MAC filtering is disabled, you cannot use the Port / MAC filtering facility until all the conflicting settings have been changed in the Port / MAC filter, VLAN or permanent MAC address entry.

A.5.6.5 Port–port Relationships Versus Standard MAC Entries

A port relationship takes priority over a regular MAC entry. A filter for a standard MAC address can only accept destination ports that are a subset of the port–port relationship entry.

A.6 IP (Internet Protocol)

The switch uses IP for management. You need to configure the switch's IP parameters if:

- The switch is to be configured / managed over the network from a boot server or network management system
- You want to use SNMP management
- You want to be able to establish a TELNET session to Local Management over the network

A.6.1 IP Addresses

A.6.1.1 Address Assignment

An IP address consists of two parts: network and host (or local) address. The network part must be globally unique and is assigned by InterNIC (International Network Information Center). The host address is the responsibility of the network manager.

In private networks, where connections to other IP networks are not available, locally assigned IP addresses can be used.

A.6.1.2 Frame Types and Type Codes

The following Ethernet type codes are used in the IP environment:

Table A.5 - Frame Types and Codes

Type field	Description
0800	DOD Internet Protocol (IP)
0806	Address Resolution Protocol

A.6.1.3 IP Address Structure

A.6.1.3.1 Address Notation

IP addresses are 32-bit numbers. The most common notation for IP addresses divides the 32-bit address into four 8-bit fields and specifies the value of each field as a decimal number (from `0` to `255`, each representing an 8-bit octet). Each number field is separated by a period (for example, 14.0.65.3). This is called the dotted decimal notation.

A.6.1.3.2 Network Numbers

The 32-bit address field consists of a network and a local host part. They are divided into different address classes which differ in the number of bits allocated to the network part and the host part (local address) of the address. The value of the first octet in the IP address defines the address class (classes A, B, C, D).

A.6.1.3.3 Class A Address

The class A address comprises a 7-bit network number and a 24-bit host address. The highest order bit is set to `0`. This allows 126 class A networks.

Table A.6 - Class A Addresses

1								2								3								4							
7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
0	Network							Host Address																							

A.6.1.3.4 Class B Address

The class B address comprises a 14-bit network number and a 16-bit host address. The two highest-order bits are set to `1 0`. This allows 16256 class B networks.

Table A.7 - Class B Addresses

1								2								3								4							
7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
10	Network															Host Address															

A.6.1.3.5 Class C Address

The class C address comprises a 21-bit network number and a 8-bit host address. The three highest-order bits are set to `1 1 0`. This allows 2072640 class C networks.

Table A.8 - Class C Addresses

1								2								3								4							
7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
1 1 0			Network																					Host Address							

A.6.1.3.6 Class D Address

The class D address is used as a multicast address. The four highest-order bits are set to `1 1 1 0`.

Table A.9 - Class D Addresses

1								2								3								4							
7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
1 1 1 0				Multicast Address																											

NOTE

No addresses are allowed which have the four highest-order bits set to 1 1 1 1 (also known as class E address).

A.6.1.3.7 Addresses Available

The following IP addresses are available for the different IP address classes:

n = network part of the address,
h = host part of the address.

Table A.10 - Address Ranges by Class

Class	Address Range available	Notation
A	1.0.0.0 through 126.0.0.0 (127.h.h.h reserved)	n.h.h.h
B	128.0.0.0 through 191.254.0.0	n.n.h.h
C	192.0.0.0 through 223.255.254.0	n.n.n.h
D	224.0.0.0 through 239.255.255.255 for multicasts.	n.n.n.n
E	240.0.0.0 through 247.255.255.255 reserved.	n.n.n.n

A.6.1.3.8 IP Address Class Overview

The table below summarizes the different classes of IP address:

Table A.11 - IP Address Class Summary

	Class A	Class B	Class C
Max. no. of networks	127	16256	2072640
Max. no. of computers per network	16777214	65534	254
Network no. part	First field	First two fields	First three fields
Network no. range	001 to 127	128 000 to 191 255	192 000 000 to 223 255 255
Host no. part	Last three fields	Last two fields	Last field
Host no. range	000 000 001 to 255 255 254	001 001 to 255 254	001 to 254

A.7 Spanning Tree

You can change the:

- Priority given to the switch
- Maximum length of time information is retained by the switch
- Time between transmitted Configuration BPDUs
- Time the switch spends in the Listening and Learning states

A.7.1 Warning When Using VLANs

It is important to be aware of problems that may arise when using Spanning Tree and VLANs. The Spanning Tree can use alternative paths (such as different ports) to get messages to their destination. VLANs specify which ports can receive messages.

WARNING!

When using the Spanning Tree facility, only use one VLAN. Using two or more VLANs may cause unexpected alterations in your network topology.

A.7.2 Spanning Tree Protocol

A.7.2.1 Spanning Tree Protocol Concept

Since alternative paths are desirable for backup and other purposes, IEEE and ISO have proposed a standard to solve the problem of “network loops”. The solution is called “The Spanning Tree Protocol”, and is described in IEEE document 802.1D, “Local MAC Bridges”.

A.7.2.2 Bridging Loops

Within the Spanning Tree Algorithm, switches connected in a LAN must detect potential “bridge loops”, and then remove these loops by blocking the appropriate ports to other switches. This is illustrated in the following diagram:

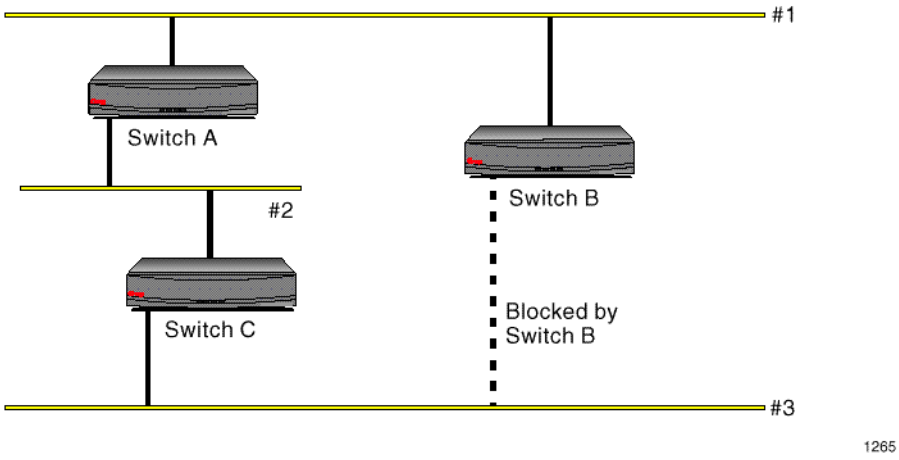


Figure A.2 - Spanning Tree and Bridge Loops

An alternate path has been established by connecting Switch B in parallel with Switches A and C — this also creates a potential bridge loop. However, by using the Spanning Tree Algorithm, Switch B breaks the loop and blocks its path to segment 3.

A.7.2.3 Bridge Failure

If Switch A fails, the Spanning Tree Algorithm must be capable of activating an alternative path, such as Switch B.

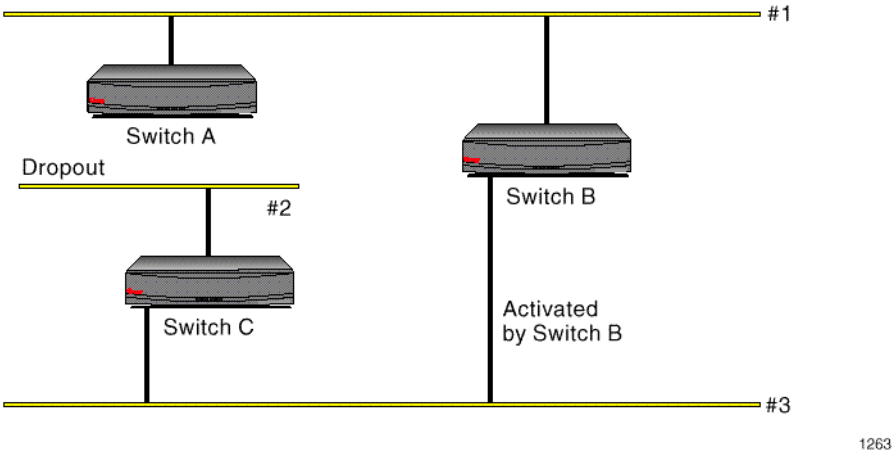


Figure A.3 - Spanning Tree and Bridge Failures

A.7.2.4 Network Extension

If the network is extended by adding Switch D, the Spanning Tree Algorithm must be capable of adapting automatically to the new topology, that is Switch B stops looping by blocking the path to segment 3.

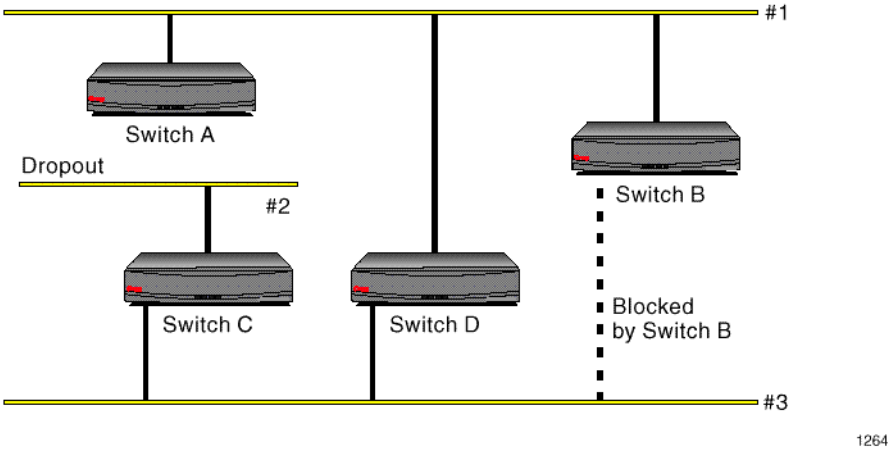


Figure A.4 - Spanning Tree Adapting to New Topology

A.7.2.5 Port States When Enabled

Each switch is identified by a switch ID, and each port (interface) on a switch is identified by a Port ID.

Ports can be either disabled or enabled. Ports which are enabled can be in one of the following states:

Listening Switches send messages to one another to establish the network topology and the optimal paths to the different segments of the network. Other data is not transmitted.

Blocking The switch enters the Blocking State if a path with higher priority is found to exist during the Listening State. Normal data is not transmitted.

Learning The switch enters the Learning State if no path with a higher priority is found during the Listening State. Learned entries are entered in the Unicast Destination Forwarding Table. Normal data is not transmitted.

Forwarding The switch enters the Forwarding State after having been in the Learning State for a predefined time period. Normal data is transmitted.

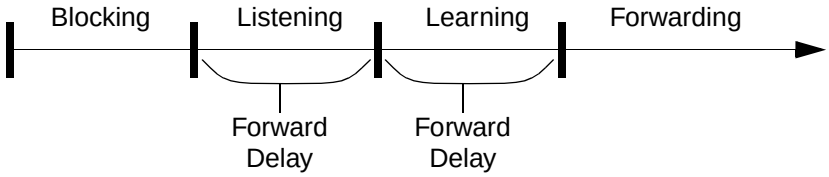


Figure A.5 - Port States

A.7.2.6 Disabled Ports

Ports which are disabled do not adapt to solve the problem network loops using the Spanning Tree Protocol.

A.7.2.7 Spanning Tree Topology

The cost factor is used to calculate the distance from each port of a switch to the Root Switch. On the basis of this, each port on a switch is assigned one of the following states:

Root Port The port that is closest to the Root Switch. Only one port on each switch is assigned as the Root Port.

Designated Port The ports that connect to switches further away from the Root Switch than the switch. The Root Switch only has Designated Ports.

Blocking If any ports are not assigned a Root Port or a Designated Port State, they are assigned a "Blocking" State. Frames (with the exception of Configuration BPDUs) are not accepted or transmitted by the port when it is in the Blocking State. The port can be said to be in stand-by.

A.7.2.8 Frame Propagation

By enforcing this strict hierarchy and by only forwarding frames between Root Ports and Designated Ports, the possibility of bridging loops is removed.

Frames cannot be sent directly between switches (except via the Root Switch).

A.7.2.9 7-hop Limit

In addition to the strict bridging hierarchy imposed by the Spanning Tree Algorithm, a 7-hop limit is introduced. Frames should not pass more than 7 bridges and this limits the size of the bridged network.

A.7.2.10 Configuration BPDU Messages

To establish the stable paths, each switch sends Configuration BPDU Frames to its neighboring switches. These Configuration BPDU messages contain information about the spanning tree topology. The contents of these frames only changes when the bridged network topology changes or has not been established.

A.7.2.11 Configuration BPDU Message Propagation

When a bridged network is in a stable condition, switches continue to send Configuration BPDU Frames to its neighboring switches at regular intervals. Configuration BPDU Frames are transmitted down the spanning tree from Designated Ports to Root Ports. If a Configuration BPDU is not received by the Root Port on a switch in a predefined time interval (for example, because a switch along the path has dropped out), the port enters the Listening State to redetermine its stable path.

A.7.2.12 MAC Address Ageing

MAC address ageing is overruled by changes in the Spanning Tree. When the Spanning Tree is bridging and blocking, the topology of the network can change. This means the MAC addresses are changing and the Spanning Tree overrides the set MAC address ageing value.

A.8 Permanent Address Assignments

You can:

- See which ports have MAC addresses permanently attached to them
- Specify if other addresses are allowed to use individual ports
- Specify a permanent (locked) MAC address for each port
- Delete user addresses from the port list

A.8.1 Permanent Explanation

A.8.1.1 Address Table

The switch learns the topology of the network by matching the address of the station (which sent the incoming frame) to the port on which it arrived. In this way it compiles an address table of which stations are connected to each port.

Once an address is learned, a frame destined for that address is forwarded only on the port to which it is attached. The switch removes "old" entries from the table to ensure that the address table is always kept up-to-date.

A.8.1.2 Permanent Address

You can make stations permanent on a port so that they are never removed from the switch's address table regardless of how long they have been quiet.

Print servers are a good example of silent network devices — they are not able to send packets to the switch and the MAC address is never learned by the switch.

A.8.1.3 Why Make Addresses Permanent?

If the switch receives a frame with an unknown destination address, it sends (or "floods") the frame out on all ports. You can reduce flooding by specifying permanent addresses on a port; these addresses are not removed regardless of how long they have been quiet.

You can allow only the defined MAC address(es) for a port to be able to use that port, thus increasing security by preventing the intrusion of unknown devices.

Unfortunately, defining permanent addresses on the ports can reduce your network's ability to move stations from one port location to another.

A.9 VLANs (Virtual LANs)

The use of VLANs lets you:

- Create separate user groups
- Easily relocate people (and their PCs) within the building
- Limit broadcast and multicast traffic
- Increase security because the groups can not communicate with each other

A.9.1 Policy-based VLAN

These VLANs can be created based on the following policies:

- Ports
- IP addresses
- IP subnets
- MAC addresses
- Any combination of the four policies above

A.9.2 Warning When Using VLANs

It is important to be aware of problems that may arise when using Spanning Tree and VLANs. The Spanning Tree can use alternative paths (such as different ports) to get messages to their destination. VLANs specify which ports can receive messages.

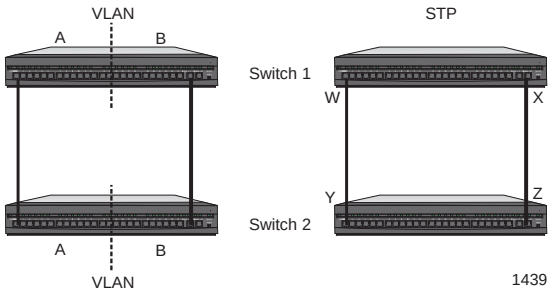


Figure A.6 - Spanning Tree and VLANs

In the above diagram, we have two switches. To the left, we see the two switches connected and the ports are grouped in two VLANs: A and B. On the right, we have enabled STP; STP blocks the path between X and Z (to avoid looping) and, therefore, destroys the VLAN setup (because the VLAN needs these ports to receive messages).

A.9.3 VLAN Explanation

You can create separate VLANs by assigning port numbers of the switch, IP addresses of devices, IP subnets and MAC addresses to a VLAN on the switch. This effectively "cuts" the switch into completely independent segments. VLANs are useful for:

- Security issues. Groups can be isolated and the group traffic can be prevented from being switched to other groups.
- Limiting Broadcast and Multicast traffic on the network to the specific VLAN.
- Resource allocation (departmental vs. common resources). Certain groups can be allocated to specific resources, such as servers.
- Application specific reasons, for example to provide firewall protection.

If you have a network that is subnetted, you can configure the switch's VLANs to match the number of subnets you have created. You can then use routers to connect the subnets and provide filtering and firewall protection.

A.9.3.1 Membership of VLANs

It is important to note that a device can be a member of more than one VLAN. Any conflict in membership between the VLANs can be checked using Stack View.

A.9.3.2 Designated Management VLAN

On the switch, there is always one VLAN that is designated to manage via SNMP. This VLAN cannot be deleted unless another is selected as the Designated Management VLAN.

A.9.3.3 IP Learning

There are some ports you will only want to use the IP policy — not port or MAC address policies. This is called IP learning, and to ensure this happens the port can be selected to support IP learning.

Glossary

10Base-T - a 10 Mbps baseband Ethernet specification utilizing twisted-pair cabling (Category 3, 4, or 5). 10BaseT, which is part of the IEEE 802.3 specification, has a distance limit of approximately 100 meters per segment.

802.1d Spanning Tree Bridging - the IEEE standard for bridging; a MAC layer standard for transparently connecting two or more LANs (often called subnetworks) that are running the same protocols and cabling. This arrangement creates an extended network, in which any two workstations on the linked LANs can share data.

802.3 Ethernet - the IEEE standard for Ethernet; a physical-layer standard that uses the CSMA / CD access method on a bus-topology LAN.

802.5 Token Ring - the IEEE physical-layer standard that uses the token-passing access method on a ring-topology LAN.

AAL Connection - an association established by the AAL between two or more next higher layer entities.

Adapter - A fitting that supplies a passage between two sets of equipment when they cannot be directly interconnected.

Adaptive Differential Pulse Code Modulation (ADPCM) - A technique that allows analog voice signals to be carried on a 32K bps digital channel. Sampling is done at 8Hz with 4 bits used to describe the difference between adjacent samples.

Adaptive Pulse Code Modulation (APCM) - A technique that effectively reduces occupied bandwidth per active speaker by reducing sampling rates during periods of overflow peak traffic.

Address - A unique identity of each network station on a LAN or WAN.

Address Complete Message (ACM) - A B-ISUP call control message from the receiving exchange to sending exchange indicating the completion of address information.

Address Mask - a bit mask used to identify which bits in an address (usually an IP address) are network significant, subnet significant, and host significant portions of the complete address. This mask is also known as the subnet mask because the subnetwork portion of the address can be determined by comparing the binary version of the mask to an IP address in that subnet. The mask holds the same number of bits as the protocol address it references.

Address Prefix - A string of 0 or more bits up to a maximum of 152 bits that is the lead portion of one or more ATM addresses.

Address Resolution - The procedure by which a client associates a LAN destination with the ATM address of another client or the BUS.

Address Resolution Protocol (ARP) - a method used to resolve higher level protocol addressing (such as IP) into the appropriate header data required for ATM; i.e., port, VPI, and VCI; also defines the AAL type to be used.

Agent - a component of network- and desktop-management software, such as SNMP, that gathers information from MIBs.

alarm - an unsolicited message from a device, typically indicating a problem with the system that requires attention.

Alarm Indication Signal (AIS) - In T1, an all ones condition used to alert a receiver that its incoming signal (or frame) has been lost. The loss of signal or frame is detected at the receiving end, and the failed signal is replaced by all the ones condition which the receiver interprets as an AIS. The normal response to this is AIS is for the receiving end to generate a yellow alarm signal as part of its transmission towards the faulty end. (The AIS itself is sometimes called a Blue Signal).

A-Law - The PCM coding and companding standard used in Europe.

Allowable Cell Rate (ACR) - parameter defined by the ATM Forum for ATM traffic management. ACR varies between the MCR and the PCR, and is dynamically controlled using congestion control mechanisms.

Alternate Mark Inversion (AMI) - A line coding format used on T1 facilities that transmits ones by alternate positive and negative pulses.

Alternate Routing - A mechanism that supports the use of a new path after an attempt to set up a connection along a previously selected path fails.

American National Standards Institute (ANSI) - a private organization that coordinates the setting and approval of some U.S. standards. It also represents the United States to the International Standards Organization.

American Standard Code for Information Interchange (ASCII) - a standard character set that (typically) assigns a 7-bit sequence to each letter, number, and selected control characters.

AppleTalk - a networking protocol developed by Apple Computer for communication between Apple's products and other computers. Independent of the network layer, AppleTalk runs on LocalTalk, EtherTalk and TokenTalk.

Application Layer - Layer seven of the ISO reference model; provides the end-user interface.

Application Program (APP) - a complete, self-contained program that performs a specific function directly for the user.

Application Program Interface (API) - a language format that defines how a program can be made to interact with another program, service, or other software; it allows users to develop custom interfaces with FORE products.

Assigned Cell - a cell that provides a service to an upper layer entity or ATM Layer Management entity (ATMM-entity).

asxmon - a FORE program that repeatedly displays the state of the switch and its active ports.

Asynchronous Time Division Multiplexing (ATDM) - a multiplexing technique in which a transmission capability is organized into a priori, unassigned time slots. The time slots are assigned to cells upon request of each application's instantaneous real need.

Asynchronous Transfer Mode (ATM) - a transfer mode in which the information is organized into cells. It is asynchronous in the sense that the recurrence of cells containing information from an individual user is not necessarily periodic.

ATM Adaptation Layer (AAL) - the AAL divides user information into segments suitable for packaging into a series of ATM cells. AAL layer types are used as follows:

AAL-1 - constant bit rate, time-dependent traffic such as voice and video
AAL-2 - still undefined; a placeholder for variable bit rate video transmission
AAL-3/4 - variable bit rate, delay-tolerant data traffic requiring some sequencing and/or error detection support (originally two AAL types, connection-oriented and connectionless, which have been combined)
AAL-5 - variable bit rate, delay-tolerant, connection-oriented data traffic requiring minimal sequencing or error detection support

ATM Address - Defined in the UNI Specification as 3 formats, each having 20 bytes in length.

ATM Forum - an international non-profit organization formed with the objective of accelerating the use of ATM products and services through a rapid convergence of interoperability specifications. In addition, the Forum promotes industry cooperation and awareness.

ATM Inverse Multiplexing (AIMUX) - A device that allows multiple T1 or E1 communications facilities to be combined into a single broadband facility for the transmission of ATM cells.

ATM Layer link - a section of an ATM Layer connection between two adjacent active ATM Layer entities (ATM-entities).

ATM Link - a virtual path link (VPL) or a virtual channel link (VCL).

ATM Management Interface (AMI) - the user interface to FORE Systems' *ForeThought* switch control software (SCS). AMI lets users monitor and change various operating configurations of FORE Systems switches and network module hardware and software, IP connectivity, and SNMP network management.

ATM Peer-to-Peer Connection - a virtual channel connection (VCC) or a virtual path connection (VPC) directly established, such as workstation-to-workstation. This setup is not commonly used in networks.

ATM Traffic Descriptor - a generic list of parameters that can be used to capture the intrinsic traffic characteristics of a requested ATM connection.

ATM User-to-User Connection - an association established by the ATM Layer to support communication between two or more ATM service users (i.e., between two or more next higher layer entities or between two or more ATM entities). The communication over an ATM Layer connection may be either bidirectional or unidirectional. The same Virtual Channel Identifier (VCI) is used for both directions of a connection at an interface.

atmarp - a FORE program that shows and manipulates ATM ARP entries maintained by the given device driver. This is also used to establish PVC connections.

ATM-attached Host Functional Group (AHFG) - The group of functions performed by an ATM-attached host that is participating in the MPOA service.

atmconfig - a FORE program used to enable or disable SPANS signaling.

atmstat - a FORE program that shows statistics gathered about a given adapter card by the device driver. These statistics include ATM layer and ATM adaptation layer cell and error counts. This can also be used to query other hosts via SNMP.

Attachment User Interface (AUI) - IEEE 802.3 interface between a media attachment unit (MAU) and a network interface card (NIC). The term AUI can also refer to the rear panel port to which an AUI cable might attach.

Auto-logout - a feature that automatically logs out a user if there has been no user interface activity for a specified length of time.

Automatic Protection Switching (APS) - Equipment installed in communications systems to detect circuit failures and automatically switch to redundant, standby equipment.

Available Bit Rate (ABR) - a type of traffic for which the ATM network attempts to meet that traffic's bandwidth requirements. It does not guarantee a specific amount of bandwidth and the end station must retransmit any information that did not reach the far end.

Backbone - the main connectivity device of a distributed system. All systems that have connectivity to the backbone connect to each other, but systems can set up private arrangements with each other to bypass the backbone to improve cost, performance, or security.

Backplane - High-speed communications line to which individual components are connected.

Backward Explicit Congestion Notification (BECN) - A Resource Management cell type generated by the network or the destination, indicating congestion or approaching congestion for traffic flowing in the direction opposite that of the BECN cell.

Bandwidth - usually identifies the capacity or amount of data that can be sent through a given circuit; may be user-specified in a PVC.

Baud - unit of signalling speed, equal to the number of discrete conditions or signal events per second. If each signal event represents only one bit, the baud rate is the same as bps; if each signal event represents more than one bit (such as a dibit), the baud rate is smaller than bps.

Bayonet-Neill-Concelman (BNC) - a bayonet-locking connector used to terminate coaxial cables. BNC is also referred to as Bayonet Network Connector.

Bipolar 8 Zero Substitution (B8ZS) - a technique used to satisfy the ones density requirements of digital T-carrier facilities in the public network while allowing 64 Kbps clear channel data. Strings of eight consecutive zeroes are replaced by an eight-bit code representing two intentional bipolar pulse code violations (000V10V1).

Bipolar Violation (BPV) - an error event on a line in which the normal pattern of alternating high (one) and low (zero) signals is disrupted. A bipolar violation is noted when two high signals occur without an intervening low signal, or vice versa.

B-ISDN Inter-Carrier Interface (B-ICI) - An ATM Forum defined specification for the interface between public ATM networks to support user services across multiple public carriers.

Bit Error Rate (BER) - A measure of transmission quality, generally shown as a negative exponent, (e.g., 10^{-7} which means 1 out of 10^{7} bits [1 out of 10,000,000 bits] are in error).

Bit Interleaved Parity (BIP) - an error-detection technique in which character bit patterns are forced into parity, so that the total number of one bits is always odd or always even. This is accomplished by the addition of a one or zero bit to each byte, as the byte is transmitted; at the other end of the transmission, the receiving device verifies the parity (odd or even) and the accuracy of the transmission.

Bit Robbing - The use of the least significant bit per channel in every sixth frame for signaling.

Bit Stuffing - A process in bit-oriented protocols where a zero is inserted into a string of ones by the sender to prevent the receiver from interpreting valid user data (the string of ones) as control characters (a Flag character for instance).

Border Gateway Protocol (BGP) - used by gateways in an internet connecting autonomous networks. It is derived from experiences learned using the EGP.

bps - bits per second

Bridge - a device that expands a Local Area Network by forwarding frames between data link layers associated with two separate cables, usually carrying a common protocol. Bridges can usually be made to filter certain packets (to forward only certain traffic).

Bridge Protocol Data Unit (BPDU) - A message type used by bridges to exchange management and control information.

Broadband - a service or system requiring transmission channels capable of supporting rates greater than the Integrated Services Digital Network (ISDN) primary rate.

Broadband Access - an ISDN access capable of supporting one or more broadband services.

Broadband Connection Oriented Bearer (BCOB) - Information in the SETUP message that indicates the type of service requested by the calling user.

BCOB-A (Bearer Class A) - Indicated by ATM end user in SETUP message for connection-oriented, constant bit rate service. The network may perform internetworking based on AAL information element (IE).

BCOB-C (Bearer Class C) - Indicated by ATM end user in SETUP message for connection-oriented, variable bit rate service. The network may perform internetworking based on AAL information element (IE).

BCOB-X (Bearer Class X) - Indicated by ATM end user in SETUP message for ATM transport service where AAL, traffic type and timing requirements are transparent to the network.

Broadband Integrated Services Digital Network (B-ISDN) - a common digital network suitable for voice, video, and high-speed data services running at rates beginning at 155 Mbps.

Broadband ISDN User's Part (B-ISUP) - A protocol used to establish, maintain and release broadband switched network connections across an SS7 / ATM network.

Broadband Terminal Equipment (B-TE) - An equipment category for B-ISDN which includes terminal adapters and terminals.

Broadcast - Data transmission to all addresses or functions.

Broadcast and Unknown Server (BUS) - in an emulated LAN, the BUS is responsible for accepting broadcast, multicast, and unknown unicast packets from the LECs to the broadcast MAC address (FFFFFFFFFFFF) via dedicated point-to-point connections, and forwarding the packets to all of the members of the ELAN using a single point-to-multipoint connection.

Brouter (bridging/router) - a device that routes some protocols and bridges others based on configuration information.

Buffer - A data storage medium used to compensate of a difference in rate of data flow or time of occurrence of events when transmitting data from one device to another.

Building Integrated Timing Supply (BITS) - a master timing supply for an entire building, which is a master clock and its ancillary equipment. The BITS supplies DS1 and / or composite clock timing references for synchronization to all other clocks and timing sources in that building.

Bursty Errored Seconds (BES) - a BES contains more than 1 and fewer than 320 path coding violation error events, and no severely errored frame or AIS defects. Controlled slips are not included in determining BESs.

Bursty Second - a second during which there were at least the set number of BES threshold event errors but fewer than the set number of SES threshold event errors.

Byte - A computer-readable group of bits (normally 8 bits in length).

Call - an association between two or more users or between a user and a network entity that is established by the use of network capabilities. This association may have zero or more connections.

Carrier - a company, such as any of the "baby Bell" companies, that provide network communications services, either within a local area or between local areas.

Carrier Group Alarm (CGA) - A service alarm generated by a channel bank when an out-of-frame (OOF) condition exists for some predetermined length of time (generally 300 milliseconds to 2.5 seconds). The alarm causes the calls using a trunk to be dropped and trunk conditioning to be applied.

Carrier Identification Parameter (CIP) - A 3 or 4 digit code in the initial address message identifying the carrier to be used for the connection.

cchan - a FORE program that manages virtual channels on a *ForeRunner* switch running `asxd`.

Cell - an ATM Layer protocol data unit (PDU). The basic unit of information transported in ATM technology, each 53-byte cell contains a 5-byte header and a 48-byte payload.

Cell Delay Variation (CDV) - a quantification of cell clumping for a connection. The cell clumping CDV (yk) is defined as the difference between a cell's expected reference arrival time (ck) and its actual arrival time (ak). The expected reference arrival time (ck) of cell k of a specific connection is max. T is the reciprocal of the negotiated peak cell rate.

Cell Delineation - the protocol for recognizing the beginning and end of ATM cells within the raw serial bit stream.

Cell Header - ATM Layer protocol control information.

Cell Loss Priority (CLP) - the last bit of byte four in an ATM cell header; indicates the eligibility of the cell for discard by the network under congested conditions. If the bit is set to 1, the cell may be discarded by the network depending on traffic conditions.

Cell Loss Ratio - In a network, cell loss ratio is (1-x/y), where y is the number of cells that arrive in an interval at an ingress of the network; and x is the number of these y cells that leave at the egress of the network element.

Cell Loss Ratio (CLR) - CLR is a negotiated QoS parameter and acceptable values are network specific. The objective is to minimize CLR provided the end-system adapts the traffic to the changing ATM layer transfer characteristics. The Cell Loss Ratio is defined for a connection as: Lost Cells/Total Transmitted Cells. The CLR parameter is the value of CLR that the network agrees to offer as an objective over the lifetime of the connection. It is expressed as an order of magnitude, having a range of 10-1 to 10-15 and unspecified.

Cell Misinsertion Rate (CMR) - the ratio of cells received at an endpoint that were not originally transmitted by the source end in relation to the total number of cells properly transmitted.

Cell Rate Adaptation (CRA) - a function performed by a protocol module in which empty cells (known as unassigned cells) are added to the output stream. This is because there always must be a fixed number of cells in the output direction; when there are not enough cells to transmit, unassigned cells are added to the output data stream.

Cell Relay Service (CRS) - a carrier service which supports the receipt and transmission of ATM cells between end users in compliance with ATM standards and implementation specifications.

Cell Transfer Delay - the transit delay of an ATM cell successfully passed between two designated boundaries. See CTD.

Cell Transfer Delay (CTD) - This is defined as the elapsed time between a cell exit event at the measurement point 1 (e.g., at the source UNI) and the corresponding cell entry event at the measurement point 2 (e.g., the destination UNI) for a particular connection. The cell transfer delay between two measurement points is the sum of the total inter-ATM node transmission delay and the total ATM node processing delay.

Channel - A path or circuit along which information flows.

Channel Associated Signaling (CAS) - a form of circuit state signaling in which the circuit state is indicated by one or more bits of signaling status sent repetitively and associated with that specific circuit.

Channel Bank - A device that multiplexes many slow speed voice or data conversations onto high speed link and controls the flow.

Channel Service Unit (CSU) - An interface for digital leased lines which performs loopback testing and line conditioning.

Channelization - capability of transmitting independent signals together over a cable while still maintaining their separate identity for later separation.

Circuit - A communications link between points.

Circuit Emulation Service (CES) - The ATM Forum circuit emulation service interoperability specification specifies interoperability agreements for supporting Constant Bit Rate (CBR) traffic over ATM networks that comply with the other ATM Forum interoperability agreements. Specifically, this specification supports emulation of existing TDM circuits over ATM networks.

Classical IP (CLIP) - IP over ATM which conforms to RFC 1577.

Clear to Send (CTS) - and RS-232 modem interface control signal (sent from the modem to the DTE on pin 5) which indicates that the attached DTE may begin transmitting; issuance in response to the DTE's RTS.

Clocking - Regularly timed impulses.

Closed User Group - A subgroup of network users that can be its own entity; any member of the subgroup can only communicate with other members of that subgroup.

Coaxial Cable - Coax is a type of electrical communications medium used in the LAN environment. This cable consists of an outer conductor concentric to an inner conductor, separated from each other by insulating material, and covered by some protective outer material. This medium offers large bandwidth, supporting high data rates with high immunity to electrical interference and a low incidence of errors. Coax is subject to distance limitations and is relatively expensive and difficult to install.

Cold Start Trap - an SNMP trap which is sent after a power-cycle (see *trap*).

Collision - Overlapping transmissions that occur when two or more nodes on a LAN attempt to transmit at or about the same time.

Committed Information Rate (CIR) - CIR is the information transfer rate which a network offering Frame Relay Services (FRS) is committed to transfer under normal conditions. The rate is averaged over a minimum increment of time.

Common Channel Signaling (CCS) - A form signaling in which a group of circuits share a signaling channel. Refer to SS7.

Common Management Interface Protocol (CMIP) - An ITU-TSS standard for the message formats and procedures used to exchange management information in order to operate, administer maintain and provision a network.

Concatenation - The connection of transmission channels similar to a chain.

Concentrator - a communications device that offers the ability to concentrate many lower-speed channels into and out of one or more high-speed channels.

Configuration - The phase in which the LE Client discovers the LE Service.

Congestion Management - traffic management feature that helps ensure reasonable service for VBR connections in an ATM network, based on a priority, sustained cell rate (SCR), and peak cell rate (PCR). During times of congestion, bandwidth is reduced to the SCR, based on the priority of the connection.

Connection - the concatenation of ATM Layer links in order to provide an end-to-end information transfer capability to access points.

Connection Admission Control (CAC) - the procedure used to decide if a request for an ATM connection can be accepted based on the attributes of both the requested connection and the existing connections.

Connection Endpoint (CE) - a terminator at one end of a layer connection within a SAP.

Connection Endpoint Identifier (CEI) - an identifier of a CE that can be used to identify the connection at a SAP.

Connectionless Broadband Data Service (CBDS) - A connectionless service similar to Bellcore's SMDS defined by European Telecommunications Standards Institute (ETSI).

Connectionless Service - a type of service in which no pre-determined path or link has been established for transfer of information, supported by AAL 4.

Connectionless Service (CLS) - A service which allows the transfer of information among service subscribers without the need for end-to- end establishment procedures.

Connection-Oriented Service - a type of service in which information always traverses the same pre-established path or link between two points, supported by AAL 3.

Constant Bit Rate (CBR) - a type of traffic that requires a continuous, specific amount of bandwidth over the ATM network (e.g., digital information such as video and digitized voice).

Controlled Slip (CS) - a situation in which one frame's worth of data is either lost or replicated. A controlled slip typically occurs when the sending device and receiving device are not using the same clock.

Convergence Sublayer (CS) - a portion of the AAL. Data is passed first to the CS where it is divided into rational, fixed-length packets or PDUs (Protocol Data Units). For example, AAL 4 processes user data into blocks that are a maximum of 64 kbytes long.

Corresponding Entities - peer entities with a lower layer connection among them.

cpath - a FORE program used to manage virtual paths on a *ForeRunner* switch running asxd.

cport - a FORE program that monitors and changes the state of ports on a *ForeRunner* switch running asxd.

Cross Connection - a mapping between two channels or paths at a network device.

Customer Premise Equipment (CPE) - equipment that is on the customer side of the point of demarcation, as opposed to equipment that is on a carrier side. See also point of demarcation.

Cut Through - Establishment of a complete path for signaling and / or audio communications.

Cyclic Redundancy Check (CRC) - an error detection scheme in which a number is derived from the data that will be transmitted. By recalculating the CRC at the remote end and comparing it to the value originally transmitted, the receiving node can detect errors.

D3/D4 - Refers to compliance with AT&T TR (Technical Reference) 62411 definitions for coding, supervision, and alarm support. D3 / D4 compatibility ensures support of digital PBXes, M24 services, Megacom services, and Mode 3 D3 / D4 channel banks at DS-1 level.

D4 Channelization - refers to compliance with AT&T Technical Reference 62411 regarding DS1 frame layout (the sequential assignment of channels and time slot numbers within the DS1).

D4 Framed/Framing Format - in T1, a 193-bit frame format in which the 193rd bit is used for framing and signaling information (the frame / framing bit). To be considered in support of D4 Framing, a device must be able to synchronize and frame-up on the 193rd bit.

Data Communications Equipment (DCE) - a definition in the RS232C standard that describes the functions of the signals and the physical characteristics of an interface for a communication device such as a modem.

Data Country Code (DCC) - This specifies the country in which an address is registered. The codes are given in ISO 3166. The length of this field is two octets. The digits of the data country code are encoded in Binary Coded Decimal (BCD) syntax. The codes will be left justified and padded on the right with the hexadecimal value “F” to fill the two octets.

Data Link - Communications connection used to transmit data from a source to a destination.

Data Link Connection Identifier (DLCI) - connection identifier associated with frame relay packets that serves the same functions as, and translates directly to, the VPI / VCI on an ATM cell.

Data Link Layer - Layer 2 of the OSI model, responsible for encoding data and passing it to the physical medium. The IEEE divides this layer into the LLC (Logical Link Control) and MAC (Media Access Control) sublayers.

Data Set Ready (DSR) - an RS-232 modem interface control signal (sent from the modem to the DTE on pin 6) which indicates that the modem is connected to the telephone circuit. Usually a prerequisite to the DTE issuing RTS.

Data Terminal Equipment (DTE) - generally user devices, such as terminals and computers, that connect to data circuit-terminating equipment. They either generate or receive the data carried by the network.

Data Terminal Ready (DTR) - an RS232 modem interface control signal (sent from the DTE to the modem on pin 20) which indicates that the DTE is ready for data transmission and which requests that the modem be connected to the telephone circuit.

Datagram - a packet of information used in a connectionless network service that is routed to its destination using an address included in the datagram's header.

DECnet - Digital Equipment Corporation's proprietary LAN.

Defense Advanced Research Projects Agency (DARPA) - the US government agency that funded the ARPANET.

Demultiplexing - a function performed by a layer entity that identifies and separates SDUs from a single connection to more than one connection (see *multiplexing*).

Destination End Station (DES) - An ATM termination point which is the destination for ATM messages of a connection and is used as a reference point for ABR services. See SES.

Digital Access and Cross-Connect System (DACS) - Digital switching system for routing T1 lines, and DS-0 portions of lines, among multiple T1 ports.

Digital Cross-connect System (DCS) - an electronic patch panel used to route digital signals in a central office.

Digital Standard n (0, 1, 1C, 2, and 3) (DSn) - a method defining the rate and format of digital hierarchy, with asynchronous data rates defined as follows:

DS0	64kb / s	1 voice channel
DS1	1.544Mb / s	24 DS0s
DS1C	3.152 Mb / s	2 DS1s
DS2	6.312 Mb / s	4 DS1s
DS3	44.736 Mb / s	28 DS1s

Synchronous data rates (SONET) are defined as:

STS-1 / OC-1	51.84 Mb / s	28 DS1s or 1 DS3
STS-3 / OC-3	155.52 Mb / s	3 STS-1s byte interleaved
STS-3c / OC-3c	155.52 Mb / s	Concatenated, indivisible payload
STS-12 / OC-12	622.08 Mb / s	12 STS-1s, 4 STS-3cs, or any mixture
STS-12c / OC-12c	622.08 Mb / s	Concatenated, indivisible payload
STS-48 / OC-48	2488.32 Mb / s	48 STS-1s, 16 STS-3cs, or any mixture

DIP (Dual In-line Package) Switch - a device that has two parallel rows of contacts that let the user switch electrical current through a pair of those contacts to on or off. They are used to reconfigure components and peripherals.

Domain Name Server - a computer that converts names to their corresponding Internet numbers. It allows users to telnet or FTP to the name instead of the number.

Domain Naming System (DNS) - the distributed name and address mechanism used in the Internet.

Duplex - Two way communication.

DXI - a generic phrase used in the full names of several protocols, all commonly used to allow a pair of DCE and DTE devices to share the implementation of a particular WAN protocol. The protocols define the packet formats used to transport data between DCE and DTE devices.

DXI Frame Address (DFA) - a connection identifier associated with ATM DXI packets that serves the same functions as, and translates directly to, the VPI/VCI on an ATM cell.

Dynamic Allocation - A technique in which the resources assigned for program execution are determined by criteria applied at the moment of need.

E.164 - A public network addressing standard utilizing up to a maximum of 15 digits. ATM uses E.164 addressing for public network addressing.

E1 - Wide-area digital transmission scheme used predominantly in Europe that carries data at a rate of 2.048 Mbps. E1 lines can be leased for private use from common carriers.

E3 - Wide-area digital transmission scheme used predominantly in Europe that carries data at a rate of 34.368 Mbps. E3 lines can be leased for private use from common carriers.

Edge Device - A physical device which is capable of forwarding packets between legacy interworking interfaces (e.g., Ethernet, Token Ring, etc.) and ATM interfaces based on data-link and network layer information but which does not participate in the running of any network layer routing protocol. An Edge Device obtains forwarding descriptions using the route distribution protocol.

elarp - a FORE program that shows and manipulates MAC and ATM address mappings for LAN Emulation Clients (LECs).

elconfig - a FORE program that shows and modifies LEC configuration. Lets the user set the NSAP address of the LAN Emulation Configuration Server, display the list of Emulated LANs configured in the LECS for this host, display the list of ELANs locally configured along with the membership state of each, and locally administer ELAN membership.

Electrically Erasable Programmable Read Only Memory (EEPROM) - an EPROM that can be cleared with electrical signals rather than the traditional ultraviolet light.

Electromagnetic Interference (EMI) - signals generated and radiated by an electronic device that cause interference with radio communications, among other effects.

Electronics Industries Association (EIA) - a USA trade organization that issues its own standards and contributes to ANSI; developed RS-232. Membership includes USA manufacturers.

Embedded SNMP Agent - an SNMP agent can come in two forms: embedded or proxy. An embedded SNMP agent is integrated into the physical hardware and software of the unit.

Emulated Local Area Network (ELAN) - A logical network initiated by using the mechanisms defined by LAN Emulation. This could include ATM and legacy attached end stations.

End System (ES) - a system where an ATM connection is terminated or initiated (an originating end system initiates the connection; a terminating end system terminates the connection).

End System Identifier (ESI) - This identifier distinguishes multiple nodes at the same level in case the lower level peer group is partitioned.

End-to-End Connection - when used in reference to an ATM network, a connection that travels through an ATM network, passing through various ATM devices and with endpoints at the termination of the ATM network.

Enterprise - Terminology generally referring to customers with multiple, non-contiguous geographic locations.

Equalization (EQL) - the process of compensating for line distortions.

Erasable Programmable Read Only Memory (EPROM) - A PROM which may be erased and rewritten to perform new or different functions (normally done with a PROM burner).

Errored Second (ES) - a second during which at least one code violation occurred.

Ethernet - a 10-Mbps, coaxial standard for LANs in which all nodes connect to the cable where they contend for access.

Excessive Zeroes (EXZ) Error Event - An Excessive Zeroes error event for an AMI-coded signal is the occurrence of more than fifteen contiguous zeroes. For a B8ZS coded signal, the defect occurs when more than seven contiguous zeroes are detected.

Explicit Forward Congestion Indication (EFCI) - the second bit of the payload type field in the header of an ATM cell, the EFCI bit indicates network congestion to receiving hosts. On a congested switch, the EFCI bit is set to “1” by the transmitting network module when a certain number of cells have accumulated in the network module's shared memory buffer. When a cell is received that has its EFCI bit set to “1,” the receiving host notifies the sending host, which should then reduce its transmission rate.

Explicit Rate (ER) - The Explicit Rate is an RM-cell field used to limit the source ACR to a specific value. It is initially set by the source to a requested rate (such as PCR). It may be subsequently reduced by any network element in the path to a value that the element can sustain. ER is formatted as a rate.

Extended Industry Standard Architecture (EISA) - bus architecture for desktop computers that provides a 32-bit data passage and maintains compatibility with the ISA or AT architecture.

Extended Super Frame (ESF) - a T1 framing format that utilizes the 193rd bit as a framing bit, but whose Superframe is made up of 24 frames instead of 12 as in D4 format. ESF also provides CRC error detection and maintenance data link functions.

Exterior Gateway Protocol (EGP) - used by gateways in an internet, connecting autonomous networks.

Fairness - related to Generic Flow Control, fairness is defined as meeting all of the agreed quality of service requirements by controlling the order of service for all active connections.

Far End Block Error (FEBE) - an error detected by extracting the 4-bit FEBE field from the path status byte (G1). The legal range for the 4-bit field is between 0000 and 1000, representing zero to eight errors. Any other value is interpreted as zero errors.

Far End Receive Failure (FERF) - a line error asserted when a 110 binary pattern is detected in bits 6, 7, 8 of the K2 byte for five consecutive frames. A line FERF is removed when any pattern other than 110 is detected in these bits for five consecutive frames.

Far-End - in a relationship between two devices in a circuit, the far-end device is the one that is remote.

Face Contact (FC) - Designation for fiber optic connector designed by Nippon Telegraph and Telephone which features a movable anti-rotation key allowing good repeatable performance despite numerous mating. Normally referred to as Fiber Connector, FC actually stands for Face Contact and sometimes linked with PC (Point Contact), designated as FC or FC-PC.

FCC Part 68 - The FCC rules regulating the direct connection of non-telephone company provided equipment to the public telephone network.

Federal Communications Commission (FCC) - a board of commissioners appointed by the President under the Communications Act of 1934, with the authority to regulate all interstate telecommunications originating in the United States, including transmission over phone lines.

Fiber Distributed Data Interface (FDDI) - high-speed data network that uses fiber-optic as the physical medium. Operates in similar manner to Ethernet or Token Ring, only faster.

File Transfer Protocol (FTP) - a TCP/IP protocol that lets a user on one computer access, and transfer data to and from, another computer over a network. ftp is usually the name of the program the user invokes to accomplish this task.

First-In, First-Out (FIFO) - method of coordinating the sequential flow of data through a buffer.

Flag - a bit pattern of six binary "1"s bounded by a binary "0" at each end (forms a 0111 1110 or Hex "7E"). It is used to mark the beginning and/or end of a frame.

Flow Control - The way in which information is controlled in a network to prevent loss of data when the receiving buffer is near its capacity.

***ForeThought* PNNI (FT-PNNI) -** a FORE Systems routing and signalling protocol that uses private ATM (NSAP) addresses; a precursor to ATM Forum PNNI (see PNNI).

Forward Error Correction (FEC) - A technique used by a receiver for correcting errors incurred in transmission over a communications channel without requiring retransmission of any information by the transmitter; typically involves a convolution of the transmitted bits and the appending of extra bits by both the receiver and transmitter using a common algorithm.

Forward Explicit Congestion Notification (FECN) - Bit set by a Frame Relay network to inform data terminal equipment (DTE) receiving the frame that congestion was experienced in the path from source to destination. DTE receiving frames with the FECN bit set can request that higher-level protocols take flow control action as appropriate.

Fractional T1 - the use of bandwidth in 64Kbps increments up to 1.544Mbps from a T1 facility.

Frame - a variable length group of data bits with a specific format containing flags at the beginning and end to provide demarcation.

Frame Check Sequence (FCS) - In bit-oriented protocols, a 16-bit field that contains transmission error checking information, usually appended to the end of the frame.

Frame Relay - a fast packet switching protocol based on the LAPD protocol of ISDN that performs routing and transfer with less overhead processing than X.25.

Frame Synchronization Error - an error in which one or more time slot framing bits are in error.

Frame-Based UNI (FUNI) - An ATM switch-based interface which accepts frame-based ATM traffic and converts it into cells.

Frame-Relay Service (FRS) - A connection oriented service that is capable of carrying up to 4096 bytes per frame.

Framing - a protocol that separates incoming bits into identifiable groups so that the receiving multiplexer recognizes the grouping.

Frequency Division Multiplexing (FDM) - a method of dividing an available frequency range into parts with each having enough bandwidth to carry one channel.

Gbps - gigabits per second (billion)

Generic Cell Rate Algorithm (GCRA) - an algorithm which is employed in traffic policing and is part of the user / network service contract. The GCRA is a scheduling algorithm which ensures that cells are marked as conforming when they arrive when expected or later than expected and non-conforming when they arrive sooner than expected.

Generic Connection Admission Control (GCAC) - This is a process to determine if a link has potentially enough resources to support a connection.

Generic Flow Control (GFC) - the first four bits of the first byte in an ATM cell header. Used to control the flow of traffic across the User-to-Network Interface (UNI), and thus into the network. Exact mechanisms for flow control are still under investigation and no explicit definition for this field exists at this time. (This field is used only at the UNI; for NNI-NNI use (between network nodes), these four bits provide additional network address capacity, and are appended to the VPI field.)

GIO - a proprietary bus architecture used in certain Silicon Graphics, Inc. workstations.

Header - protocol control information located at the beginning of a protocol data unit.

Header Error Control (HEC) - a CRC code located in the last byte of an ATM cell header that is used for checking cell header integrity only.

High Density Bipolar (HDB3) - A bipolar coding method that does not allow more than 3 consecutive zeroes.

High Level Data Link Control (HDLC) - An ITU-TSS link layer protocol standard for point-to-point and multi-point communications.

High Performance Parallel Interface (HIPPI) - ANSI standard that extends the computer bus over fairly short distances at speeds of 800 and 1600 Mbps.

High-Speed Serial Interface (HSSI) - a serial communications connection that operates at speeds of up to 1.544 Mbps.

Host - In a network, the primary or controlling computer in a multiple computer installation.

HPUX - the Hewlett-Packard version of UNIX.

Hub - a device that connects several other devices, usually in a star topology.

I/O Module - FORE's interface cards for the LAX-20 LAN Access Switch, designed to connect Ethernet, Token Ring, and FDDI LANs to *ForeRunner* ATM networks.

Institute of Electrical and Electronics Engineers (IEEE) - the world's largest technical professional society. Based in the U.S., the IEEE sponsors technical conferences, symposia & local meetings worldwide, publishes nearly 25% of the world's technical papers in electrical, electronics & computer engineering, provides educational programs for members, and promotes standardization.

IEEE 802 - Standards for the interconnection of LAN computer equipment. Deals with the Data Link Layers of the ISO Reference Model for OSI.
IEEE 802.1 - Defines the high-level network interfaces such as architecture, internetworking and network management.
IEEE 802.2 - Defines the Logical Link Control interface between the Data Link and Network Layers.
IEEE 802.3 - Defines CSMA / CD (Ethernet).
IEEE 802.4 - Defines the token-passing bus.
IEEE 802.5 - Defines the Token Ring access methodology. This standard incorporates IBM's Token Ring specifications.
IEEE 802.6 - Defines Metropolitan Area Networks.
IEEE 802.7 - The broadband technical advisory group.
IEEE 802.8 - The fiber optics technical advisory group.
IEEE 802.9 - Defines integrated data and voice networks.

Integrated Services Digital Network (ISDN) - an emerging technology that is beginning to be offered by the telephone carriers of the world. ISDN combines voice and digital network services into a single medium or wire.

Interexchange Carriers (IXC) - Long-distance communications companies that provide service between Local Access Transport Areas (LATAs).

Interface Data - the unit of information transferred to / from the upper layer in a single interaction across a SAP. Each Interface Data Unit (IDU) controls interface information and may also contain the whole or part of the SDU.

Interface Data Unit (IDU) - The unit of information transferred to / from the upper layer in a single interaction across the SAP. Each IDU contains interface control information and may also contain the whole or part of the SDU.

Interim Local Management Interface (ILMI) - the standard that specifies the use of the Simple Network Management Protocol (SNMP) and an ATM management information base (MIB) to provide network status and configuration information.

Intermediate System (IS) - a system that provides forwarding functions or relaying functions or both for a specific ATM connection. OAM cells may be generated and received.

International Standards Organization (ISO) - a voluntary, non treaty organization founded in 1946 that is responsible for creating international standards in many areas, including computers and communications.

International Telephone and Telegraph Consultative Committee (CCITT) - the international standards body for telecommunications.

Internet - (note the capital "I") the largest internet in the world including large national backbone nets and many regional and local networks worldwide. The Internet uses the TCP/IP suite. Networks with only e-mail connectivity are not considered on the Internet.

internet - while an internet is a network, the term "internet" is usually used to refer to a collection of networks interconnected with routers.

Internet Addresses - the numbers used to identify hosts on an internet network. Internet host numbers are divided into two parts; the first is the network number and the second, or local, part is a host number on that particular network. There are also three classes of networks in the Internet, based on the number of hosts on a given network. Large networks are classified as Class A, having addresses in the range 1-126 and having a maximum of 16,387,064 hosts. Medium networks are classified as Class B, with addresses in the range 128-191 and with a maximum of 64,516 hosts. Small networks are classified as Class C, having addresses in the range 192-254 with a maximum of 254 hosts. Addresses are given as dotted decimal numbers in the following format:

nnn.nnn.nnn.nnn

In a Class A network, the first of the numbers is the network number, the last three numbers are the local host address.

In a Class B network, the first two numbers are the network, the last two are the local host address.

In a Class C network, the first three numbers are the network address, the last number is the local host address.

The following table summarizes the classes and sizes:

Class	First #	Max# Hosts
A	1-126	16,387,064
B	129-191	64,516
C	192-223	254

Network mask values are used to identify the network portion and the host portion of the address. Default network masks are as follows:

Class A - 255.0.0.0

Class B - 255.255.0.0

Class C - 255.255.255.0

Subnet masking is used when a portion of the host ID is used to identify a subnetwork. For example, if a portion of a Class B network address is used for a subnetwork, the mask could be set as 255.255.255.0. This would allow the third byte to be used as a subnetwork address. All hosts on the network would still use the IP address to get on the Internet.

Internet Control Message Protocol (ICMP) - the protocol that handles errors and control messages at the IP layer. ICMP is actually a part of the IP protocol layer. It can generate error messages, test packets, and informational messages related to IP.

Internet Engineering Task Force (IETF) - a large, open, international community of network designers, operators, vendors and researchers whose purpose is to coordinate the operation, management and evolution of the Internet to resolve short- and mid-range protocol and architectural issues.

Internet Protocol (IP) - a connectionless, best-effort packet switching protocol that offers a common layer over dissimilar networks.

Internetwork Packet Exchange (IPX) Protocol - a NetWare protocol similar to the Xerox Network Systems (XNS) protocol that provides datagram delivery of messages.

Interoperability - The ability of software and hardware on multiple machines, from multiple vendors, to communicate.

Interworking Function (IWF) - provides a means for two different technologies to interoperate.

IP Address - a unique 32-bit integer used to identify a device in an IP network. You will most commonly see IP addresses written in "dot" notation (e.g., 192.228.32.14).

IP Netmask - a 32-bit pattern that is combined with an IP address to determine which bits of an IP address denote the network number and which denote the host number. Netmasks are useful for sub-dividing IP networks. IP netmasks are written in "dot" notation (e.g., 255.255.0.0).

ISA Bus - a bus standard developed by IBM for expansion cards in the first IBM PC. The original bus supported a data path only 8 bits wide. IBM subsequently developed a 16-bit version for its AT class computers. The 16-bit AT ISA bus supports both 8- and 16-bit cards. The 8-bit bus is commonly called the PC/XT bus, and the 16-bit bus is called the AT bus.

Isochronous - signals carrying embedded timing information or signals that are dependent on uniform timing; usually associated with voice and/or video transmission.

International Telecommunications Union Telecommunications (ITU-T) - an international body of member countries whose task is to define recommendations and standards relating to the international telecommunications industry. The fundamental standards for ATM have been defined and published by the ITU-T (Previously CCITT).

J2 - Wide-area digital transmission scheme used predominantly in Japan that carries data at a rate of 6.312 Mbps.

Jitter - analog communication line distortion caused by variations of a signal from its reference timing position.

Joint Photographic Experts Group (JPEG) - An ISO Standards group that defines how to compress still pictures.

Jumper - a patch cable or wire used to establish a circuit, often temporarily, for testing or diagnostics; also, the devices, shorting blocks, used to connect adjacent exposed pins on a printed circuit board that control the functionality of the card.

Kbps - kilobits per second (thousand)

LAN Access Concentrator - a LAN access device that allows a shared transmission medium to accommodate more data sources than there are channels currently available within the transmission medium.

LAN Emulation Address Resolution Protocol (LE_ARP) - A message issued by a LE client to solicit the ATM address of another function.

LAN Emulation Client (LEC) - the component in an end system that performs data forwarding, address resolution, and other control functions when communicating with other components within an ELAN.

LAN Emulation Configuration Server (LECS) - the LECS is responsible for the initial configuration of LECs. It provides information about available ELANs that a LEC may join, together with the addresses of the LES and BUS associated with each ELAN.

LAN Emulation Server (LES) - the LES implements the control coordination function for an ELAN by registering and resolving MAC addresses to ATM addresses.

LAN Emulation (LANE) - technology that allows an ATM network to function as a LAN backbone. The ATM network must provide multicast and broadcast support, address mapping (MAC-to-ATM), SVC management, and a usable packet format. LANE also defines Ethernet and Token Ring ELANs.

lane - a program that provides control over the execution of the LAN Emulation Server (LES), Broadcast / Unknown Server (BUS), and LAN Emulation Configuration Server (LECS) on the local host.

Latency - The time interval between a network station seeking access to a transmission channel and that access being granted or received.

Layer Entity - an active layer within an element.

Layer Function - a part of the activity of the layer entities.

Layer Service - a capability of a layer and the layers beneath it that is provided to the upper layer entities at the boundary between that layer and the next higher layer.

Layer User Data - the information transferred between corresponding entities on behalf of the upper layer or layer management entities for which they are providing services.

le - a FORE program that implements both the LAN Emulation Server (LES) and the Broadcast / Unknown Server (BUS).

Leaky Bucket - informal cell policing term for the Generic Cell Rate Algorithm which in effect receives cells into a bucket and leaks them out at the specified or contracted rate (i.e., PCR).

Least Significant Bit (LSB) - lowest order bit in the binary representation of a numerical value.

lecs - a FORE program that implements the assignment of individual LECs to different emulated LANs.

leq - a FORE program that provides information about an ELAN. This information is obtained from the LES, and includes MAC addresses registered on the ELAN together with their corresponding ATM addresses.

Line Build Out (LBO) - Because T1 circuits require the last span to lose 15-22.5 dB, a selectable output attenuation is generally required of DTE equipment (typical selections include 0.0, 7.5 and 15 dB of loss at 772 KHz).

Line Code Violations (LCV) - Error Event. A Line Coding Violation (LCV) is the occurrence of either a Bipolar Violation (BPV) or Excessive Zeroes (EXZ) Error Event.

Link - An entity that defines a topological relationship (including available transport capacity) between two nodes in different subnetworks. Multiple links may exist between a pair of subnetworks. Synonymous with logical link.

Link Access Procedure, Balanced (LAPB) - Data link protocol in the X.25 protocol stack. LAPB is a bit-oriented protocol derived from HDLC. See also HDLC and X.25.

Link Down Trap - an SNMP trap, sent when an interface changes from a normal state to an error state, or is disconnected.

Link Layer - layer in the OSI model regarding transmission of data between network nodes.

Link Up Trap - an SNMP trap, sent when an interface changes from an error condition to a normal state.

Load Sharing - Two or more computers in a system that share the load during peak hours. During periods of non peak hours, one computer can manage the entire load with the other acting as a backup.

Local Access and Transport Area (LATA) - Geographic boundaries of the local telephone network, specified by the FCC, in which a single LEC may perform its operations. Communications outside or between LATAs are provided by IXCs.

Local Area Network (LAN) - a data network intended to serve an area of only a few square kilometers or less. Because the network is known to cover only a small area, optimizations can be made in the network signal protocols that permit higher data rates.

Logical Link Control (LLC) - protocol developed by the IEEE 802 committee for data-link-layer transmission control; the upper sublayer of the IEEE Layer 2 (OSI) protocol that complements the MAC protocol; IEEE standard 802.2; includes end-system addressing and error checking.

Loopback - a troubleshooting technique that returns a transmitted signal to its source so that the signal can be analyzed for errors. Typically, a loopback is set at various points in a line until the section of the line that is causing the problem is discovered.

looptest - program that tests an interface for basic cell reception and transmission functionality, usually used for diagnostic purposes to determine if an interface is functioning properly.

Loss Of Frame (LOF) - a type of transmission error that may occur in wide-area carrier lines.

Loss Of Pointer (LOP) - a type of transmission error that may occur in wide-area carrier lines.

Loss Of Signal (LOS) - a type of transmission error that may occur in wide-area carrier lines, or a condition declared when the DTE senses a loss of a DS1 signal from the CPE for more the 150 milliseconds (the DTE generally responds with an all ones “Blue or AIS” signal).

Management Information Base (MIB) - the set of parameters that an SNMP management station can query or set in the SNMP agent of a networked device (e.g., router).

Maximum Burst Size (MBS) - the Burst Tolerance (BT) is conveyed through the MBS which is coded as a number of cells. The BT together with the SCR and the GCRA determine the MBS that may be transmitted at the peak rate and still be in conformance with the GCRA.

Maximum Burst Tolerance - the largest burst of data that a network device is guaranteed to handle without discarding cells or packets. Bursts of data larger than the maximum burst size may be subject to discard.

Maximum Cell Delay Variance (MCDV) - This is the maximum two-point CDV objective across a link or node for the specified service category.

Maximum Cell Loss Ratio (MCLR) - This is the maximum ratio of the number of cells that do not make it across the link or node to the total number of cells arriving at the link or node.

Maximum Cell Transfer Delay (MCTD) - This is the sum of the fixed delay component across the link or node and MCDV.

Maximum Transmission Unit (MTU) - the largest unit of data that can be sent over a type of physical medium.

Mbps - megabits per second (million)

Media Access Control (MAC) - a media-specific access control protocol within IEEE 802 specifications; currently includes variations for Token Ring, token bus, and CSMA/CD; the lower sublayer of the IEEE’s link layer (OSI), which complements the Logical Link Control (LLC).

Media Attachment Unit (MAU) - device used in Ethernet and IEEE 802.3 networks that provides the interface between the AUI port of a station and the common medium of the Ethernet. The MAU, which can be built into a station or can be a separate device, performs physical layer functions including conversion of the digital data from the Ethernet interface, collision detection, and injection of bits onto the network.

Media Interface Connector (MIC) - fiber optic connector that joins fiber to the FDDI controller.

Message Identifier (MID) - message identifier used to associate ATM cells that carry segments from the same higher layer packet.

Metasignalling - an ATM Layer Management (LM) process that manages different types of signalling and possibly semipermanent virtual channels (VCs), including the assignment, removal, and checking of VCs.

Metasignalling VCs - the standardized VCs that convey metasignalling information across a User-to-Network Interface (UNI).

Metropolitan Area Network (MAN) - network designed to carry data over an area larger than a campus such as an entire city and its outlying area.

MicroChannel - a proprietary 16- or 32-bit bus developed by IBM for its PS/2 computers' internal expansion cards; also offered by others.

Minimum Cell Rate (MCR) - parameter defined by the ATM Forum for ATM traffic management, defined only for ABR transmissions and specifying the minimum value for the ACR.

Most Significant Bit (MSB) - highest order bit in the binary representation of a numerical value.

Motion Picture Experts Group (MPEG) - ISO group dealing with video and audio compression techniques and mechanisms for multiplexing and synchronizing various media streams.

MPOA Client - A device which implements the client side of one or more of the MPOA protocols, (i.e., is a SCP client and/or an RDP client. An MPOA Client is either an Edge Device Functional Group (EDFG) or a Host Behavior Functional Group (HBFG).

MPOA Server - An MPOA Server is any one of an ICFG or RSFG.

MPOA Service Area - The collection of server functions and their clients. A collection of physical devices consisting of an MPOA server plus the set of clients served by that server.

MPOA Target - A set of protocol address, path attributes, (e.g., internetwork layer QoS, other information derivable from received packet) describing the intended destination and its path attributes that MPOA devices may use as lookup keys.

Mu-Law - The PCM coding and companding standard used in Japan and North America.

Multicasting - The ability to broadcast messages to one node or a select group of nodes.

Multi-homed - a device having both an ATM and another network connection, like Ethernet.

Multimode Fiber Optic Cable (MMF) - fiber optic cable in which the signal or light propagates in multiple modes or paths. Since these paths may have varying lengths, a transmitted pulse of light may be received at different times and smeared to the point that pulses may interfere with surrounding pulses. This may cause the signal to be difficult or impossible to receive. This pulse dispersion sometimes limits the distance over which a MMF link can operate.

Multiplexing - a function within a layer that interleaves the information from multiple connections into one connection (see demultiplexing).

Multipoint Access - user access in which more than one terminal equipment (TE) is supported by a single network termination.

Multipoint-to-Multipoint Connection - a collection of associated ATM VC or VP links, and their associated endpoint nodes, with the following properties:

1. All N nodes in the connection, called Endpoints, serve as a Root Node in a Point-to-Multipoint connection to all of the (N-1) remaining endpoints.

2. Each of the endpoints can send information directly to any other endpoint, but the receiving endpoint cannot distinguish which of the endpoints is sending information without additional (e.g., higher layer) information.

Multipoint-to-Point Connection - a Point-to-Multipoint Connection may have zero bandwidth from the Root Node to the Leaf Nodes, and non-zero return bandwidth from the Leaf Nodes to the Root Node. Such a connection is also known as a Multipoint-to-Point Connection.

Multiprotocol over ATM (MPOA) - An effort taking place in the ATM Forum to standardize protocols for the purpose of running multiple network layer protocols over ATM.

Narrowband Channel - sub-voicegrade channel with a speed range of 100 to 200 bps.

National TV Standards Committee (NTSC) - Started in the US in 1953 from a specification laid down by the National Television Standards Committee. It takes the B-Y and R-Y color difference signals, attenuates them to I and Q, then modulates them using double-sideband suppressed subcarrier at 3.58MHz. The carrier reference is sent to the receiver as a burst during the back porch. An industry group that defines how television signals are encoded and transmitted in the US. (See also PAL, SECAM for non-U.S. countries).

Near-End - in a relationship between two devices in a circuit, the near-end device is the one that is local.

Network Layer - Layer three In the OSI model, the layer that is responsible for routing data across the network.

Network Management Entity (NM) - body of software in a switching system that provides the ability to manage the PNNI protocol. NM interacts with the PNNI protocol through the MIB.

Network Management Layer (NML) - an abstraction of the functions provided by systems which manage network elements on a collective basis, providing end-to-end network monitoring.

Network Management Station (NMS) - system responsible for managing a network or portion of a network by talking to network management agents, which reside in the managed nodes.

Network Module - ATM port interface cards which may be individually added to or removed from any *ForeRunner* ATM switch to provide a diverse choice of connection alternatives.

Network Parameter Control (NPC) - Defined as the set of actions taken by the network to monitor and control traffic from the NNI. Its main purpose is to protect network resources from malicious as well as unintentional misbehavior which can affect the QoS of other already established connections by detecting violations of negotiated parameters and taking appropriate actions. Refer to UPC.

Network Redundancy - Duplicated network equipment and/or data which can provide a backup in case of network failures.

Network Service Access Point (NSAP) - OSI generic standard for a network address consisting of 20 octets. ATM has specified E.164 for public network addressing and the NSAP address structure for private network addresses.

Network-to-Network Interface or Network Node Interface (NNI) - the interface between two public network pieces of equipment.

Node - A computer or other device when considered as part of a network.

Non Return to Zero (NRZ) - a binary encoding scheme in which ones and zeroes are represented by opposite and alternating high and low voltages and where there is no return to a zero (reference) voltage between encoded bits.

Non Return to Zero Inverted (NRZI) - A binary encoding scheme that inverts the signal on a "1" and leaves the signal unchanged for a "0". (Also called transition encoding.)

Nonvolatile Storage - Memory storage that does not lose its contents when power is turned off.

NuBus - a high-speed bus used in Macintosh computers, structured so users can put a card into any slot on the board without creating conflict over the priority between those cards.

nx64K - This refers to a circuit bandwidth or speed provided by the aggregation of nx64 kbps channels (where n= integer > 1). The 64K or DS0 channel is the basic rate provided by the T Carrier systems.

Nyquist Theorem - In communications theory, a formula stating that two samples per cycle is sufficient to characterize a bandwidth limited analog signal; in other words, the sampling rate must be twice the highest frequency component of the signal (i.e., sample 4 KHz analog voice channels 8000 times per second).

Object Identifier (OID) - the address of a MIB variable.

Octet - a grouping of 8 bits; similar, but not identical to, a byte.

One's Density - The requirement for digital transmission lines in the public switched telephone network that eight consecutive "0"s cannot be in a digital data stream; exists because repeaters and clocking devices within the network will lose timing after receiving eight "0"s in a row; a number of techniques are used to insert a "1" after every seventh-consecutive "0" (see Bit Stuffing).

Open Shortest Path First (OSPF) Protocol - a routing algorithm for IP that incorporates least-cost, equal-cost, and load balancing.

Open Systems Interconnection (OSI) - the 7-layer suite of protocols designed by ISO committees to be the international standard computer network architecture.

OpenView - Hewlett-Packard's network management software.

Operation and Maintenance (OAM) Cell - a cell that contains ATM LM information. It does not form part of the upper layer information transfer.

Optical Carrier level-n (OC-n) - The optical counterpart of STS-n (the basic rate of 51.84 Mbps on which SONET is based is referred to as OC-1 or STS-1).

Organizationally Unique Identifier (OUI) - Part of RFC 1483. A three-octet field in the SubNetwork Attachment Point (SNAP) header, identifying an organization which administers the meaning of the following two octet Protocol Identifier (PID) field in the SNAP header. Together they identify a distinct routed or bridged protocol.

Out-of-Band Management - refers to switch configuration via the serial port or over Ethernet, not ATM.

Out-of-Frame (OOF) - a signal condition and alarm in which some or all framing bits are lost.

Packet - An arbitrary collection of data grouped and transmitted with its user identification over a shared facility.

Packet Assembler Disassembler (PAD) - interface device that buffers data sent to/from character mode devices, and assembles and disassembles the packets needed for X.25 operation.

Packet Internet Groper (ping) - a program used to test reachability of destinations by sending them an ICMP echo request and waiting for a reply.

Packet Level Protocol (PLP) - Network layer protocol in the X.25 protocol stack. Sometimes called X.25 Level 3 or X.25 Protocol.

Packet Switched Network (PSN) - a network designed to carry data in the form of packets. The packet and its format is internal to that network.

Packet Switching - a communications paradigm in which packets (messages) are individually routed between hosts with no previously established communications path.

Payload Scrambling - a technique that eliminates certain bit patterns that may occur within an ATM cell payload that could be misinterpreted by certain sensitive transmission equipment as an alarm condition.

Payload Type (PT) - bits 2...4 in the fourth byte of an ATM cell header. The PT indicates the type of information carried by the cell. At this time, values 0...3 are used to identify various types of user data, values 4 and 5 indicate management information, and values 6 and 7 are reserved for future use.

Peak Cell Rate - at the PHY Layer SAP of a point-to-point VCC, the Peak Cell Rate is the inverse of the minimum inter-arrival time T0 of the request to send an ATM-SDU.

Peak Cell Rate (PCR) - parameter defined by the ATM Forum for ATM traffic management. In CBR transmissions, PCR determines how often data samples are sent. In ABR transmissions, PCR determines the maximum value of the ACR.

Peer Entities - entities within the same layer.

Peripheral Component Interconnect (PCI) - a local-bus standard created by Intel.

Permanent Virtual Channel Connection (PVCC) - A Virtual Channel Connection (VCC) is an ATM connection where switching is performed on the VPI/VCI fields of each cell. A Permanent VCC is one which is provisioned through some network management function and left up indefinitely.

Permanent Virtual Circuit (or Channel) (PVC) - a circuit or channel through an ATM network provisioned by a carrier between two endpoints; used for dedicated long-term information transport between locations.

Permanent Virtual Path Connection (PVPC) - A Virtual Path Connection (VPC) is an ATM connection where switching is performed on the VPI field only of each cell. A PVPC is one which is provisioned through some network management function and left up indefinitely.

Phase Alternate Line (PAL) - Largely a German/British development in the late 60s, used in the UK and much of Europe. The B-Y and R-Y signals are weighted to U and V, then modulated onto a double-sideband suppressed subcarrier at 4.43MHz. The V (R-Y) signal's phase is turned through 180 degrees on each alternate line. This gets rid of NTSC's hue changes with phase errors at the expense of de-saturation. The carrier reference is sent as a burst in the back porch. The phase of the burst is alternated every line to convey the phase switching of the V signal. The burst's average phase is -V. (see NTSC for U.S.).

Physical Layer (PHY) - the actual cards, wires, and/or fiber-optic cabling used to connect computers, routers, and switches.

Physical Layer Connection - an association established by the PHY between two or more ATM-entities. A PHY connection consists of the concatenation of PHY links in order to provide an end-to-end transfer capability to PHY SAPs.

Physical Layer Convergence Protocol (PLCP) - a framing protocol that runs on top of the T1 or E1 framing protocol.

Physical Medium (PM) - Refers to the actual physical interfaces. Several interfaces are defined including STS-1, STS-3c, STS-12c, STM-1, STM-4, DS1, E1, DS2, E3, DS3, E4, FDDI-based, Fiber Channel-based, and STP. These range in speeds from 1.544Mbps through 622.08 Mbps.

Physical Medium Dependent (PMD) - a sublayer concerned with the bit transfer between two network nodes. It deals with wave shapes, timing recovery, line coding, and electro-optic conversions for fiber based links.

Plesiochronous - two signals are plesiochronous if their corresponding significant instants occur at nominally the same rate, with variations in rate constrained to specified limits.

Point of Demarcation - the dividing line between a carrier and the customer premise that is governed by strict standards that define the characteristics of the equipment on each side of the demarcation. Equipment on one side of the point of demarcation is the responsibility of the customer. Equipment on the other side of the point of demarcation is the responsibility of the carrier.

Point-to-Multipoint Connection - a collection of associated ATM VC or VP links, with associated endpoint nodes, with the following properties:

1. One ATM link, called the Root Link, serves as the root in a simple tree topology. When the Root node sends information, all of the remaining nodes on the connection, called Leaf nodes, receive copies of the information.

2. Each of the Leaf Nodes on the connection can send information directly to the Root Node. The Root Node cannot distinguish which Leaf is sending information without additional (higher layer) information. (See the following note for Phase 1.)

3. The Leaf Nodes cannot communicate directly to each other with this connection type.

Note: Phase 1 signalling does not support traffic sent from a Leaf to the Root.

Point-to-Point Connection - a connection with only two endpoints.

Point-to-Point Protocol (PPP) - Provides a method for transmitting packets over serial point-to-point links.

Policing - the function that ensures that a network device does not accept traffic that exceeds the configured bandwidth of a connection.

Port Identifier - The identifier assigned by a logical node to represent the point of attachment of a link to that node.

Presentation Layer - Sixth layer of the OSI model, providing services to the application layer.

Primary Reference Source (PRS) - Equipment that provides a timing signal whose long-term accuracy is maintained at 1 x 10 -11 or better with verification to universal coordinated time (UTC) and whose timing signal is used as the basis of reference for the control of other clocks within a network.

Primitive - an abstract, implementation-independent interaction between a layer service user and a layer service provider.

Priority - the parameter of ATM connections that determines the order in which they are reduced from the peak cell rate to the sustained cell rate in times of congestion. Connections with lower priority (4 is low, 1 is high) are reduced first.

Private Branch Exchange (PBX) - a private phone system (switch) that connects to the public telephone network and offers in-house connectivity. To reach an outside line, the user must dial a digit like 8 or 9.

Private Network Node Interface or Private Network-to-Network Interface (PNNI) - a protocol that defines the interaction of private ATM switches or groups of private ATM switches

Programmable Read-Only Memory (PROM) - a chip-based information storage area that can be recorded by an operator but erased only through a physical process.

Protocol - a set of rules and formats (semantic and syntactic) that determines the communication behavior of layer entities in the performance of the layer functions.

Protocol Control Information - the information exchanged between corresponding entities using a lower layer connection to coordinate their joint operation.

Protocol Data Unit (PDU) - a unit of data specified in a layer protocol and consisting of protocol control information and layer user data.

Proxy - the process in which one system acts for another system to answer protocol requests.

Proxy Agent - an agent that queries on behalf of the manager, used to monitor objects that are not directly manageable.

Public Data Network (PDN) - a network designed primarily for data transmission and intended for sharing by many users from many organizations.

Pulse Code Modulation (PCM) - a modulation scheme that samples the information signals and transmits a series of coded pulses to represent the data.

Q.2931 - Derived from Q.93B, the narrowband ISDN signalling protocol, an ITU standard describing the signalling protocol to be used by switched virtual circuits on ATM LANs.

Quality of Service (QoS) - Quality of Service is defined on an end-to-end basis in terms of the following attributes of the end-to-end ATM connection:

Cell Loss Ratio
Cell Transfer Delay
Cell Delay Variation

Queuing Delay (QD) - refers to the delay imposed on a cell by its having to be buffered because of unavailability of resources to pass the cell onto the next network function or element. This buffering could be a result of oversubscription of a physical link, or due to a connection of higher priority or tighter service constraints getting the resource of the physical link.

Radio Frequency Interference (RFI) - the unintentional transmission of radio signals. Computer equipment and wiring can both generate and receive RFI.

Real-Time Clock - a clock that maintains the time of day, in contrast to a clock that is used to time the electrical pulses on a circuit.

Red Alarm - In T1, a red alarm is generated for a locally detected failure such as when a condition like OOF exists for 2.5 seconds, causing a CGA, (Carrier Group Alarm).

Reduced Instruction Set Computer (RISC) - a generic name for CPUs that use a simpler instruction set than more traditional designs.

Redundancy - In a data transmission, the fragments of characters and bits that can be eliminated with no loss of information.

Registration - The address registration function is the mechanism by which Clients provide address information to the LAN Emulation Server.

Relaying - a function of a layer by means of which a layer entity receives data from a corresponding entity and transmits it to another corresponding entity.

Request To Send (RTS) - an RS-232 modem interface signal (sent from the DTE to the modem on pin 4) which indicates that the DTE has data to transmit.

Requests For Comment (RFCs) - IETF documents suggesting protocols and policies of the Internet, inviting comments as to the quality and validity of those policies. These comments are collected and analyzed by the IETF in order to finalize Internet standards.

RFC1483 - Multiprotocol Encapsulation over ATM Adaptation Layer 5.
RFC1490 - Multiprotocol Interconnect over Frame Relay.
RFC1577 - Classical IP and ARP over ATM.
RFC1755 - ATM Signaling Support for IP over ATM.

Robbed-Bit Signaling - In T1, refers to the use of the least significant bit of every word of frames 6 and 12 (D4), or 6, 12, 18, and 24 (ESF) for signaling purposes.

Route Server - A physical device that runs one or more network layer routing protocols, and which uses a route query protocol in order to provide network layer routing forwarding descriptions to clients.

Router - a device that forwards traffic between networks or subnetworks based on network layer information.

Routing Domain (RD) - A group of topologically contiguous systems which are running one instance of routing.

Routing Information Protocol (RIP) - a distance vector-based protocol that provides a measure of distance, or hops, from a transmitting workstation to a receiving workstation.

Routing Protocol - A general term indicating a protocol run between routers and/or route servers in order to exchange information used to allow computation of routes. The result of the routing computation will be one or more forwarding descriptions.

SBus - hardware interface for add-in boards in later-version Sun 3 workstations.

Scalable Processor Architecture Reduced instruction set Computer (SPARC) - a powerful workstation similar to a reduced-instruction-set-computing (RISC) workstation.

Segment - a single ATM link or group of interconnected ATM links of an ATM connection.

Segmentation And Reassembly (SAR) - the SAR accepts PDUs from the CS and divides them into very small segments (44 bytes long). If the CS-PDU is less than 44 bytes, it is padded to 44 with zeroes. A two-byte header and trailer are added to this basic segment. The header identifies the message type (beginning, end, continuation, or single) and contains sequence numbering and message identification. The trailer gives the SAR-PDU payload length, exclusive of pad, and contains a CRC check to ensure the SAR-PDU integrity. The result is a 48-byte PDU that fits into the payload field of an ATM cell.

Selector (SEL) - A subfield carried in SETUP message part of ATM endpoint address Domain specific Part (DSP) defined by ISO 10589, not used for ATM network routing, used by ATM end systems only.

Semipermanent Connection - a connection established via a service order or via network management.

Serial Line IP (SLIP) - A protocol used to run IP over serial lines, such as telephone circuits or RS-232 cables, interconnecting two systems.

Service Access Point (SAP) - the point at which an entity of a layer provides services to its LM entity or to an entity of the next higher layer.

Service Data Unit (SDU) - a unit of interface information whose identity is preserved from one end of a layer connection to the other.

Service Specific Connection Oriented Protocol (SSCOP) - an adaptation layer protocol defined in ITU-T Specification: Q.2110.

Service Specific Convergence Sublayer (SSCS) - The portion of the convergence sublayer that is dependent upon the type of traffic that is being converted.

Session Layer - Layer 5 in the OSI model that is responsible for establishing and managing sessions between the application programs running in different nodes.

Severely Errored Seconds (SES) - a second during which more event errors have occurred than the SES threshold (normally 10-3).

Shaping Descriptor - *n* ordered pairs of GCRA parameters (I,L) used to define the negotiated traffic shape of an APP connection. The traffic shape refers to the load-balancing of a network, where load-balancing means configuring data flows to maximize network efficiency.

Shielded Pair - Two insulated wires in a cable wrapped with metallic braid or foil to prevent interference and provide noise free transmission.

Shielded Twisted Pair (STP) - two or more insulated wires, twisted together and then wrapped in a cable with metallic braid or foil to prevent interference and offer noise-free transmissions.

Signaling System No. 7 (SS7) - The SS7 protocol has been specified by ITU-T and is a protocol for interexchange signaling.

Simple and Efficient Adaptation Layer (SEAL) - also called AAL 5, this ATM adaptation layer assumes that higher layer processes will provide error recovery, thereby simplifying the SAR portion of the adaptation layer. Using this AAL type packs all 48 bytes of an ATM cell information field with data. It also assumes that only one message is crossing the UNI at a time. That is, multiple end-users at one location cannot interleave messages on the same VC, but must queue them for sequential transmission.

Simple Gateway Management Protocol (SGMP) - the predecessor to SNMP.

Simple Mail Transfer Protocol (SMTP) - the Internet electronic mail protocol used to transfer electronic mail between hosts.

Simple Network Management Protocol (SNMP) - the Internet standard protocol for managing nodes on an IP network.

Simple Protocol for ATM Network Signalling (SPANS) - FORE Systems' proprietary signalling protocol used for establishing SVCs between FORE Systems equipment.

Single Mode Fiber (SMF) - Fiber optic cable in which the signal or light propagates in a single mode or path. Since all light follows the same path or travels the same distance, a transmitted pulse is not dispersed and does not interfere with adjacent pulses. SMF fibers can support longer distances and are limited mainly by the amount of attenuation. Refer to MMF.

Small Computer Systems Interface (SCSI) - a standard for a controller bus that connects hardware devices to their controllers on a computer bus, typically used in small systems.

Smart PVC (SPVC) - a generic term for any communications medium which is permanently provisioned at the end points, but switched in the middle. In ATM, there are two kinds of SPVCs: smart permanent virtual path connections (SPVPCs) and smart permanent virtual channel connections (SPVCCs).

snmpd - an SMNP agent for a given adapter card.

Source - Part of communications system which transmits information.

Source Address (SA) - The address from which the message or data originated.

Source MAC Address (SA) - A six octet value uniquely identifying an end point and which is sent in an IEEE LAN frame header to indicate source of frame.

Source Traffic Descriptor - a set of traffic parameters belonging to the ATM Traffic Descriptor used during the connection set-up to capture the intrinsic traffic characteristics of the connection requested by the source.

Spanning Tree Protocol - provides loop-free topology in a network environment where there are redundant paths.

Static Route - a route that is entered manually into the routing table.

Statistical Multiplexing - a technique for allowing multiple channels and paths to share the same link, typified by the ability to give the bandwidth of a temporarily idle channel to another channel.

Stick and Click (SC) - Designation for an Optical Connector featuring a 2.5 mm physically contacting ferrule with a push-pull mating design. Commonly referred to as Structured Cabling, Structured Connectors or Stick and Click

Stick and Turn (ST) - A fiber-optic connector designed by AT&T which uses the bayonet style coupling rather than screw-on as the SMA uses. The ST is generally considered the eventual replacement for the SMA type connector.

Store-and-Forward - the technique of receiving a message, storing it until the proper outgoing line is available, then retransmitting it, with no direct connection between incoming and outgoing lines.

Straight Tip (ST) - see *Stick and Turn*.

Structured Cabling (SC) - see *Stick and Click.*

Structured Connectors (SC) - see *Stick and Click*.

Sublayer - a logical subdivision of a layer.

SubNetwork Access Protocol (SNAP) - a specially reserved variant of IEEE 802.2 encoding SNAP indicates to look further into the packet where it will fine a Type field.

Subscriber Network Interface (SNI) - the interface between an SMDS end user's CPE and the network directly serving the end user, supported by either a DS1 or DS3 access arrangement.

Super Frame (SF) - a term used to describe the repeating 12 D4 frame format that composes a standard (non-ESF) T1 service.

Super User - a login ID that allows unlimited access to the full range of a device's functionality, including especially the ability to reconfigure the device and set passwords.

Sustainable Cell Rate (SCR) - ATM Forum parameter defined for traffic management. For VBR connections, SCR determines the long-term average cell rate that can be transmitted.

Sustained Information Rate (SIR) - In ATM this refers to the long-term average data transmission rate across the User-to-Network Interface. In SMDS this refers to the committed information rate (similar to CIR for Frame Relay Service).

Switch - Equipment used to interconnect lines and trunks.

Switched Connection - A connection established via signaling.

Switched Multimegabit Data Service (SMDS) - a high-speed, datagram-based, public data network service expected to be widely used by telephone companies in their data networks.

Switched Virtual Channel Connection (SVCC) - A Switched VCC is one which is established and taken down dynamically through control signaling. A Virtual Channel Connection (VCC) is an ATM connection where switching is performed on the VPI/VCI fields of each cell.

Switched Virtual Circuit (or Channel) (SVC) - a channel established on demand by network signalling, used for information transport between two locations and lasting only for the duration of the transfer; the datacom equivalent of a dialed telephone call.

Switched Virtual Path Connection (SVPC) - a connection which is established and taken down dynamically through control signaling. A Virtual Path Connection (VPC) is an ATM connection where switching is performed on the VPI field only of each cell.

Switching System - A set of one or more systems that act together and appear as a single switch for the purposes of PNNI routing.

Symmetric Connection - a connection with the same bandwidth specified for both directions.

Synchronous - signals that are sourced from the same timing reference and hence are identical in frequency.

Synchronous Data Link Control (SDLC) - IBM's data link protocol used in SNA networks.

Synchronous Optical Network (SONET) - a body of standards that defines all aspects of transporting and managing digital traffic over optical facilities in the public network.

Synchronous Payload Envelope (SPE) - the payload field plus a little overhead of a basic SONET signal.

Synchronous Transfer Mode (STM) - a transport and switching method that depends on information occurring in regular, fixed patterns with respect to a reference such as a frame pattern.

Synchronous Transport Signal (STS) - a SONET electrical signal rate.

Systeme En Coleur Avec Memoire (SECAM) - Sequential and Memory Color Television - Started in France in the late 60s, and used by other countries with a political affiliation. This is. The B-Y and R-Y signals are transmitted on alternate lines modulated on an FM subcarrier. The memory is a one line delay line in the receiver to make both color difference signals available at the same time on all lines. Due to FM, the signal is robust in difficult terrain.

Systems Network Architecture (SNA) - a proprietary networking architecture used by IBM and IBM-compatible mainframe computers.

T1 - a specification for a transmission line. The specification details the input and output characteristics and the bandwidth. T1 lines run at 1.544 Mbps and provide for 24 data channels. In common usage, the term "T1" is used interchangeably with "DS1."

T1 Link - A wideband digital carrier facility used for transmission of digitized voice, digital data, and digitized image traffic. This link is composed of two twisted-wire pairs that can carry 24 digital channels, each operating at 64K bps at the aggregate rate of 1.544M bps, full duplex. Also referred to as DS-1.

T3 - a specification for a transmission line, the equivalent of 28 T1 lines. T3 lines run at 44.736 Mbps. In common usage, the term "T3" is used interchangeably with "DS3."

Tachometer - in *ForeView*, the tachometer shows the level of activity on a given port. The number in the tachometer shows the value of a chosen parameter in percentage, with a colored bar providing a semi-logarithmic representation of that percentage.

Tagged Cell Rate (TCR) - An ABR service parameter, TCR limits the rate at which a source may send out-of-rate forward RM-cells. TCR is a constant fixed at 10 cells / second.

Telephony - The conversion of voices and other sounds into electrical signals which are then transmitted by telecommunications media.

Telnet - a TCP / IP protocol that defines a client / server mechanism for emulating directly-connected terminal connections.

Terminal Equipment (TE) - Terminal equipment represents the endpoint of ATM connection(s) and termination of the various protocols within the connection(s).

Throughput - Measurement of the total useful information processed or communicated by a computer during a specified time period, i.e. packets per second.

Time Division Multiplexing (TDM) - a method of traditional digital multiplexing in which a signal occupies a fixed, repetitive time slot within a higher-rate signal.

Token Ring - a network access method in which the stations circulate a token. Stations with data to send must have the token to transmit their data.

topology - a program that displays the topology of a FORE Systems ATM network. An updated topology can be periodically re-displayed by use of the interval command option.

Traffic - the calls being sent and received over a communications network. Also, the packets that are sent on a data network.

Traffic Management (TM) - The traffic control and congestion control procedures for ATM. ATM layer traffic control refers to the set of actions taken by the network to avoid congestion conditions. ATM layer congestion control refers to the set of actions taken by the network to minimize the intensity, spread and duration of congestion. The following functions form a framework for managing and controlling traffic and congestion in ATM networks and may be used in appropriate combinations:

Connection Admission Control
Feedback Control
Usage Parameter Control
Priority Control
Traffic Shaping
Network Resource Management
Frame Discard
ABR Flow Control

Traffic Parameter - A parameter for specifying a particular traffic aspect of a connection.

Trailer - the protocol control information located at the end of a PDU.

Transit Delay - the time difference between the instant at which the first bit of a PDU crosses one designated boundary, and the instant at which the last bit of the same PDU crosses a second designated boundary.

Transmission Control Protocol (TCP) - a specification for software that bundles and unbundles sent and received data into packets, manages the transmission of packets on a network, and checks for errors.

Transmission Control Protocol/Internet Protocol (TCP/IP) - a set of communications protocols that has evolved since the late 1970s, when it was first developed by the Department of Defense. Because programs supporting these protocols are available on so many different computer systems, they have become an excellent way to connect different types of computers over networks.

Transmission Convergence (TC) - generates and receives transmission frames and is responsible for all overhead associated with the transmission frame. The TC sublayer packages cells into the transmission frame.

Transmission Convergence Sublayer (TCS) - This is part of the ATM physical layer that defines how cells will be transmitted by the actual physical layer.

Transparent Asynchronous Transmitter/Receiver Interface (TAXI) - Encoding scheme used for FDDI LANs as well as for ATM; supports speed typical of 100 Mbps over multimode fiber.

Transport Layer - Layer Four of the OSI reference model that is responsible for maintaining reliable end-to-end communications across the network.

trap - a program interrupt mechanism that automatically updates the state of the network to remote network management hosts. The SNMP agent on the switch supports these SNMP traps.

Trivial File Transfer Protocol (TFTP) - Part of IP, a simplified version of FTP that allows files to be transferred from one computer to another over a network.

Twisted Pair - Insulated wire in which pairs are twisted together. Commonly used for telephone connections, and LANs because it is inexpensive.

Unassigned Cells - a generated cell identified by a standardized virtual path identifier (VPI) and virtual channel identifier (VCI) value, which does not carry information from an application using the ATM Layer service.

Unavailable Seconds (UAS) - a measurement of signal quality. Unavailable seconds start accruing when ten consecutive severely errored seconds occur.

UNI 3.0/3.1 - the User-to-Network Interface standard set forth by the ATM Forum that defines how private customer premise equipment interacts with private ATM switches.

Unicasting - The transmit operation of a single PDU by a source interface where the PDU reaches a single destination.

Universal Test & Operations Interface for ATM (UTOPIA) - Refers to an electrical interface between the TC and PMD sublayers of the PHY layer.

Unshielded Twisted Pair (UTP) - a cable that consists of two or more insulated conductors in which each pair of conductors are twisted around each other. There is no external protection and noise resistance comes solely from the twists.

Unspecified Bit Rate (UBR) - a type of traffic that is not considered time-critical (e.g., ARP messages, pure data), allocated whatever bandwidth is available at any given time. UBR traffic is given a “best effort” priority in an ATM network with no guarantee of successful transmission.

Uplink - Represents the connectivity from a border node to an upnode.

Usage Parameter Control (UPC) - mechanism that ensures that traffic on a given connection does not exceed the contracted bandwidth of the connection, responsible for policing or enforcement. UPC is sometimes confused with congestion management (see *congestion management*).

User Datagram Protocol (UDP) - the TCP/IP transaction protocol used for applications such as remote network management and name-service access; this lets users assign a name, such as “RVAX*2,S,” to a physical or numbered address.

User-to-Network Interface (UNI) - the physical and electrical demarcation point between the user and the public network service provider.

V.35 - ITU-T standard describing a synchronous, physical layer protocol used for communications between a network access device and a packet network. V.35 is most commonly used in the United States and Europe, and is recommended for speeds up to 48 Kbps.

Variable Bit Rate (VBR) - a type of traffic that, when sent over a network, is tolerant of delays and changes in the amount of bandwidth it is allocated (e.g., data applications).

Virtual Channel (or Circuit) (VC) - a communications path between two nodes identified by label rather than fixed physical path.

Virtual Channel Connection (VCC) - a unidirectional concatenation of VCLs that extends between the points where the ATM service users access the ATM Layer. The points at which the ATM cell payload is passed to, or received from, the users of the ATM Layer (i.e., a higher layer or ATMM-entity) for processing signify the endpoints of a VCC.

Virtual Channel Identifier (VCI) - the address or label of a VC; a value stored in a field in the ATM cell header that identifies an individual virtual channel to which the cell belongs. VCI values may be different for each data link hop of an ATM virtual connection.

Virtual Channel Link (VCL) - a means of unidirectional transport of ATM cells between the point where a VCI value is assigned and the point where that value is translated or removed.

Virtual Channel Switch - a network element that connects VCLs. It terminates VPCs and translates VCI values. The Virtual Channel Switch is directed by Control Plane functions and relays the cells of a VC.

Virtual Connection - an endpoint-to-endpoint connection in an ATM network. A virtual connection can be either a virtual path or a virtual channel.

Virtual Local Area Network (VLAN) - Work stations connected to an intelligent device which provides the capabilities to define LAN membership.

Virtual Network Software (VINES) - Banyan's network operating system based on UNIX and its protocols.

Virtual Path (VP) - a unidirectional logical association or bundle of VCs.

Virtual Path Connection (VPC) - a concatenation of VPLs between virtual path terminators (VPTs). VPCs are unidirectional.

Virtual Path Identifier (VPI) - the address or label of a particular VP; a value stored in a field in the ATM cell header that identifies an individual virtual path to which the cell belongs. A virtual path may comprise multiple virtual channels.

Virtual Path Link (VPL) - a means of unidirectional transport of ATM cells between the point where a VPI value is assigned and the point where that value is translated or removed.

Virtual Path Switch - a network element that connects VPLs, it translates VPI (not VCI) values and is directed by Control Plane functions. The Virtual Path Switch relays the cells of a Virtual Path.

Virtual Path Terminator (VPT) - a system that unbundles the VCs of a VP for independent processing of each VC.

Virtual Private Data Network (VPDN) - a private data communications network built on public switching and transport facilities rather than dedicated leased facilities such as T1s.

Virtual Private Network (VPN) - a private voice communications network built on public switching and transport facilities rather than dedicated leased facilities such as T1s.

Virtual Source/Virtual Destination (VS/VD) - An ABR connection may be divided into two or more separately controlled ABR segments. Each ABR control segment, except the first, is sourced by a virtual source. A virtual source implements the behavior of an ABR source endpoint. Backwards RM-cells received by a virtual source are removed from the connection. Each ABR control segment, except the last, is terminated by a virtual destination. A virtual destination assumes the behavior of an ABR destination endpoint. Forward RM-cells received by a virtual destination are turned around and not forwarded to the next segment of the connection.

Virtual Tributary (VT) - a structure used to carry payloads such as DS1s that run at significantly lower rates than STS-1s.

Warm Start Trap - an SNMP trap which indicates that SNMP alarm messages or agents have been enabled.

Wide-Area Network (WAN) - a network that covers a large geographic area.

Wideband Channel - Communications channel with more capacity (19.2K bps) than the standard capacity of a voice grade line.

X.21 - ITU-T standard for serial communications over synchronous digital lines. The X.21 protocol is used primarily in Europe and Japan.

X.25 - a well-established data switching and transport method that relies on a significant amount of processing to ensure reliable transport over metallic media.

Yellow Alarm - An alarm signal sent back toward the source of a failed signal due to the presence of an AIS (may be used by APS equipment to initiate switching).

Zero Byte Time Slot Interchange (ZBTSI) - A technique used with the T carrier extended superframe format (ESF) in which an area in the ESF frame carries information about the location of all-zero bytes (eight consecutive “0”s) within the data stream.

Zero Code Suppression - The insertion of a “1” bit to prevent the transmission of eight or more consecutive “0” bits. Used primarily with T1 and related digital telephone company facilities, which require a minimum “1’s density” in order to keep the individual subchannels of a multiplexed, high speed facility active.

Zero-Bit Insertion - A technique used to achieve transparency in bit-oriented protocols. A zero is inserted into sequences of one bits that cause false flag direction.

Index

P

R

S

T